# Citrix VDI-in-a-Box 5.x
## Configuring Remote Access with NetScaler Access Gateway

<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoltan Kovacs, Solutions Engineer Overview .................................. 2</td>
</tr>
<tr>
<td>Requirements ................................................................................. 2</td>
</tr>
<tr>
<td>NetScaler Resources ..................................................................... 3</td>
</tr>
<tr>
<td>Worksheet ..................................................................................... 4</td>
</tr>
<tr>
<td>VIAB Grid Configuration ................................................................. 5</td>
</tr>
<tr>
<td>AGEE Configuration ........................................................................ 7</td>
</tr>
<tr>
<td>Access Gateway Wizard ................................................................. 7</td>
</tr>
<tr>
<td>Published Applications Wizard ....................................................... 10</td>
</tr>
<tr>
<td>Configure Access Gateway Virtual Server ........................................ 11</td>
</tr>
<tr>
<td>Configure Access Gateway Policies ................................................ 12</td>
</tr>
<tr>
<td>Citrix Receiver (PNAgent) Session Policy ........................................ 14</td>
</tr>
</tbody>
</table>

### Troubleshooting

1. Q1 Have you configured the VDI-in-a-Box Grid-Wide Virtual IP? .................. 17
2. Q2 Have you configured the VDI-in-a-Box SSL Gateway? ............................... 17
3. Q3 Are you using a self-signed or valid SSL Certificate? ............................... 17
4. Q4 Is the Secure Ticket Authority (STA) server functioning? ....................... 17
5. Q5 Why are we getting the 1030 on occasion but not every time? ................. 18
6. Q6 Why won’t the VDI-in-a-Box web interface appear (page timeout or error code)? ........................................................................................................ 18
7. Q7 Why are users are prompted to type credentials twice when using a web browser? ........................................................................................................ 18
8. Q8 Can I use SmartAccess, Full VPN, or Clientless VPN with VDI-in-a-Box? .... 18
9. Q9 Can I use the NetScaler Load Balancing feature instead of the VDI-in-a-Box Grid-wide Virtual IP? ................................................................. 19
Zoltan Kovacs, Solutions Engineer Overview

This document is intended to guide customers through the configuration of Citrix NetScaler Access Gateway Enterprise Edition specifically for use with Citrix VDI-in-a-Box. As certain aspects of the VDI-in-a-Box infrastructure are different than XenApp/XenDesktop, it is important to understand and configure the AGEE accordingly. Although the same high-level concepts are the same, some configuration points and settings are different for VDI-in-a-Box.

This document assumes you already have the NetScaler product installed and configured with basic network settings. Once the NetScaler is installed (virtual or physical) and configured, you can follow this document to configure the Access Gateway.

The Access Gateway feature is the entry point users connect to in order to securely access VDI-in-a-Box desktops over the Internet. The AGEE virtual server is typically placed in the DMZ and authentication is configured on the AGEE to ensure malicious traffic does not reach the secure LAN where the VDI-in-a-Box servers and desktops reside.

The Load Balancing feature can optionally be used with VDI-in-a-Box where a single point of failure needs to be eliminated. With the current version of VDI-in-a-Box, the web interface and connection brokering roles are available on each VDI-in-a-Box server. However, if you configure the Access Gateway to point to a single server and it fails, externally users will not be able to connect. The solution is to configure the Load Balancing feature which contains a list of all the VDI-in-a-Box servers, and then configure the Access Gateway Web Interface to point to the Load Balancing server instead of VDI-in-a-Box. This configuration, along with a NetScaler HA Pair (optional), ensures High Availability of both the NetScaler and VDI-in-a-Box Web Interface & Connection Brokering. Keep in mind that external load balancers are not required for VDI-in-a-Box and even the NetScaler LB does not affect the VDI-in-a-Box back-end load balancing algorithms. It is simply used to ensure HA of the mentioned roles.

Requirements

- Citrix VDI-in-a-Box version 5.1 or later.
- NetScaler 9.2 or later. *This document is written based on NetScaler VPX 10.*
- NetScaler license. VIAB supports all paid NetScaler licenses and the VPX Express free license.
- SSL Certificate obtained from a Trusted Certificate Authority.
- Firewall Rules should allow TCP Ports 1494 (ICA) and 2598 (Session Reliability) to traverse between the Access Gateway and VDI-in-a-Box Virtual Desktops. TCP Port 443 (80 optionally if using redirection) to traverse between the WAN and the Access Gateway.
**NetScaler Resources**

If a NetScaler has not already been installed and configured, the following links can help you get started:

- NetScaler Product Home Page
- NetScaler ADC Downloads Page
- NetScaler 10 eDocs Page
- Access Gateway 10 eDocs Page
- NetScaler 9.3 Quick Start Guide
- NetScaler 9.3 Networking Guide
**Worksheet**
You can print this page to use as a quick reference guide when configuring both VDI-in-a-Box and NetScaler Access Gateway for Secure Remote Access. This worksheet will help ensure a quick and accurate deployment is achieved.

<table>
<thead>
<tr>
<th>Item</th>
<th>Your Information</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler Admin Username</td>
<td></td>
<td>Default: nsroot</td>
</tr>
<tr>
<td>NetScaler Admin Password</td>
<td></td>
<td>Default: nsroot</td>
</tr>
<tr>
<td>NetScaler Management IP</td>
<td></td>
<td>Used to access NetScaler admin console</td>
</tr>
<tr>
<td>Access Gateway Virtual IP</td>
<td></td>
<td>NetScaler Virtual IP for Access Gateway</td>
</tr>
</tbody>
</table>
| Access Gateway Fully Qualified Domain Name | | The URL users will type in to access VIAB through the Access Gateway  
Example: access.company.com |
| AD Domain Controller IP  |                  | Windows AD Domain Controller                                          |
| AD User Base DN          |                  | The AD base location to search for users                              
Example: OU=VIAB,DC=company,DC=com |
| AD Admin DN              |                  | The DN for the AD admin account                                       
Example: CN=admin,OU=VDI,DC=company,DC=com |
| AD Admin Password        |                  | Password for the AD admin account                                    |
| VIAB Grid-Wide Virtual IP|                  | VIP Configured in ViaB Advanced Properties                          |
VIAB Grid Configuration

Before configuring the NetScaler Access Gateway you will need to configure (1) Grid-wide Virtual IP for HA of the Web Interface and Connection Brokering Roles and (2) SSL Gateway Settings for STA and acceptance of connections through the gateway.

1. Logon to the VIAB grid as vdiadmin or another administrator.
2. Go to Admin > Advanced Properties menu.
3. Scroll down to the Grid section and provide an IP address in the Grid IP address field. This must be an available IP address on the network and ideally on the same subnet as the VDI-in-a-Box servers.
4. Scroll down and configure the SSL Gateway section:
   - External SSL: Type the FQDN followed by the port.
   - Internal SSL: Type the NetScaler MIP or SNIP.
5. Click **OK**. This is all you need to configure on the VIAB grid itself.
**AGEE Configuration**

**Access Gateway Wizard**

1. Right-click the Access Gateway feature and select **Enable Feature**.
2. Click the **Access Gateway wizard** link under the Getting Started section.
3. Specify the Virtual IP Address and port to use for the Access Gateway server.
4. Provide a name for the AG virtual server, such as `viab_ag_svr`.
5. Click **Next**.
6. Select an option from the **Certificate Options** menu and follow the on-screen instructions.
7. Click **Next**.
8. Type the IP address of your **DNS Server** in the Configured DNS Server field and then click Next.
9. Select an **authentication** type from the list. You can select LDAP, RADIUS, LOCAL, TACACS, or CERT. VDI-in-a-Box 5.0.x has been successfully tested to provide Single Sign-On with the Citrix Receiver when using LDAP and RADIUS pointing to
the same Active Directory domain the VDI-in-a-Box grid is pointing to. At this time Single Sign-On does not occur between the Access Gateway and VDI-in-a-Box Web Interface.

For example if using LDAP configure at a minimum the following settings:

- IP Address and Port of your Active Directory domain controller.
- Base DN (location of users) in the format of OU=VIABusers,DC=company,DC=com.
- Administrator Bind DN in the format of CN=Administrator,CN=Users,DC=company,DC=com.
- Type and Confirm the Administrator Password.
- Click Retrieve Attributes to verify connectivity from the Access Gateway to the Domain Controller. You will see a message stating Attributes from LDAP server have been retrieved successfully.

10. Click **Next**.
11. Select **Allow** for Configure Authorization.
12. Optionally enable the **Redirect to secure Web address item** if you wish to redirect requests on http (port 80) to https (port 443).
13. If redirection is enabled, fill out the **Web address** of where the redirection should occur. This should be the FQDN users will access, such as https://gateway.company.com.
14. Select **Allow users to log on using Clientless Access only**.

15. Select **Allow** for the **Clientless Access Persistent Cookie**.

16. Click **Next**, **Finish**, and then **Exit**.

17. Click the **Save** button to ensure the running configuration is saved into memory. If the configuration is not saved it will be lost if the NetScaler restarts.
Published Applications Wizard

1. Click the **Published applications wizard** link under the Getting Started section.

2. Select the **VDI-in-a-Box Access Gateway virtual server** created in the previous section from the Virtual Server Name list. Most likely you will only have one virtual server.

3. Click **Next**.

4. Type the **Web Interface Address** using the VDI-in-a-Box Grid-wide Virtual IP address, in the format of `https://10.207.83.253`. You must use **https** instead of http.

5. Type the **domain name** into the **Single Sign-on Domain** field, such as `company.com`.

6. Click **Add** in the **Secure Ticket Authority** (STA) section.

7. Type the **STA URL using the VDI-in-a-Box Grid-wide Virtual IP address**, in the format of `https://10.207.83.253/dt/sta`. You can use **http** or **https** but the path must be `/dt/sta`.

8. Click **Next**.

9. **Skip** the **Configure SmartAccess** page by clicking **Next**.

10. Click **Finish**.

11. Click the **Save** button to ensure the running configuration is saved into memory. If the configuration is not saved it will be lost if the NetScaler restarts.
Configure Access Gateway Virtual Server

1. Open the Virtual Servers menu found under the Access Gateway feature.

2. Open the VDI-in-a-Box Access Gateway virtual server.

3. Select Basic Mode.

4. Go to the Published Applications tab.
Configure Access Gateway Policies

Web Interface Session Policy
1. Open the VDI-in-a-Box Access Gateway Virtual Server.
2. Go to the Policies tab.
3. Click Insert Policy and select New Policy.
4. Provide a Name for this policy, such as viab_session_pol.
5. Select the True value from the Named Expressions list.
6. Click the Add Expression button. You will now see ns_true in the Expression field.
7. Click New in the Request Profile section.
8. Provide a Name for this Profile, such as viab_session_pro.
9. Go to the Client Experience tab.
10. Enable Override Global for Clientless Access and set to On.
11. Enable Override Global for Single Sign-on to Web Applications and check the box for the item.
12. Click the Advanced link found in Session Profile Client Experience.
13. **Enable Override Global** for Client Choices and ensure the box is NOT checked.

14. Click OK to return to the Client Experience tab.

15. **Enable Override Global** for Single Sign-on with Windows and check the box for the item.


17. **Enable Override Global** for Default Authorization Action and set to ALLOW.

18. Go to the Published Applications tab.

19. **Enable Override Global** for ICA Proxy and set to ON.

20. **Enable Override Global** for Web Interface Address and ensure the VDI-in-a-Box Grid-wide IP is in the field, such as https://10.207.83.253. You must use https and not http.

21. **Enable Override Global** for Single Sign-on Domain and ensure the domain is in the field, such as company.com.

22. Click Create for the Session Profile.

23. Click Create for the Session Policy.

24. Click Save near the top-right corner of the NetScaler web console.
Citrix Receiver (PNAgent) Session Policy
1. Open the VDI-in-a-Box Access Gateway Virtual Server.
2. Go to the Policies tab.
3. Click Insert Policy and select New Policy.
4. Provide a Name for this policy, such as viab_receiver_pol.
5. Click the Add button next to Match Any Expression.
6. Add the following express and click OK:
   Flow type: REQ
   Protocol: HTTP
   Qualifier: HEADER
   Operator: CONTAINS
   Value: CitrixReceiver
   HeaderName: User-Agent

7. Click New in the Request Profile section.
8. Provide a Name for this Profile, such as viab_receiver_pro.
9. Go to the Client Experience tab.
10. Enable Override Global for Clientless Access and set to On.
11. Enable Override Global for Single Sign-on to Web Applications and check the box for the item.
12. Click the **Advanced** link found in **Session Profile Client Experience**.
13. **Enable Override Global** for **Client Choices** and ensure the box is **NOT** checked.

14. **Click OK** to return to the **Client Experience** tab.
15. **Enable Override Global** for **Single Sign-on with Windows** and **check** the box for the item.

16. Go to the **Security** tab.
17. **Enable Override Global** for **Default Authorization Action** and set to **ALLOW**.

18. Go to the **Published Applications** tab.
19. **Enable Override Global** for **ICA Proxy** and set to **ON**.
20. **Enable Override Global** for **Web Interface Address** and add the **PNAgent path** after the **VDI-in-a-Box Grid-wide Virtual IP**, such as

   https://10.207.83.17/dt/PNAgent/config.xml

   **Note**: The PNAgent path is **CaSE-sEnsiTive**. You must also use https here.

21. **Enable Override Global** for **Single Sign-on Domain** and ensure the domain is in the field, such as **company.com**.

22. Click **Create** for the **Session Profile**.
23. Click **Create** for the **Session Policy**.
24. Verify the two policies have been created and appear in the Access Gateway Policies list.

25. Click **OK** to close the Access Gateway virtual server configuration screen.
26. Click the **Save** button near the top-right corner of the NetScaler web console.
Configuration is now complete.

Troubleshooting

The most common issue when configured the Access Gateway with VDI-in-a-Box is the 1030 error. This error appears after a user has authenticated and the ICA session is attempting to connect to the virtual desktop. This is a general connectivity issue and there are multiple root causes.

Q1 Have you configured the VDI-in-a-Box Grid-Wide Virtual IP?
A. Logon to the ViaB web console and go to the Admin > Advanced Properties menu. Go to the Grid section and type an available IP address to use as the Grid-wide virtual IP. Once saved, confirm the grid is listening for requests on that IP address by pinging it from a Command Prompt or Terminal.

Q2 Have you configured the VDI-in-a-Box SSL Gateway?
A1. Logon to the ViaB web console and go to the Admin > Advanced Properties menu. Go to the SSL Gateway section. The External Field must have the FQDN users connect; along with a port which is most cases will be 443. If the FQDN is remote.company.com on port 443, the field must be remote.company.com:443.
A2. The Internal Field will be the Mapped IP (MIP) or Subnet IP (SNIP) configured on the NetScaler. This MIP/SNIP used by the NetScaler is dependent on how you configured the NetScaler and if it is on a different subnet than the VDI-in-a-Box servers and desktops. This IP can be verified via the NetScaler web console > Network > IP section. If you encounter a connectivity error you can also log into the ViaB web console and go to the User Sessions section. Look at the Client IP address listed for the user with the failed connection. If the user went through the Access Gateway and the IP shows 10.207.83.254, then you need to ensure the Internal SSL Gateway field is 10.207.83.254. This is how VDI-in-a-Box knows to make changes to the ICA file for remote users.

Q3 Are you using a self-signed or valid SSL Certificate?
A1. If using a self-signed SSL certificate, you must install both the root and server certificate onto the end-point client in the Trusted Root Authorities store. The end-point must trust the server and root.
A2. If using a valid SSL certificate, make sure that FQDN/DNS record matches the CN (Common Name) field for the SSL Certificate. Also make sure all intermediate certificates required are linked within the NetScaler SSL Certificate section. You can validate an SSL Certificate by using the quick and easy GeoCerts SSL Checker tool at http://www.geocerts.com/ssl_checker.

Q4 Is the Secure Ticket Authority (STA) server functioning?
A. Log into the NetScaler web console, go to the Access Gateway Virtual Servers section, and open the Virtual Server created for VDI-in-a-Box remote access. Open the Published Applications tab and verify the STA server has an Identifier string and is show an UP state. If the Identifier field is empty and has a DOWN state, make sure the URL is
correct. It should start with https, use the VDI-in-a-Box Grid-wide Virtual IP, and a path of /dt/sta. If you need to make a correction just uncheck the Active box for the current entry, click Add, and type in a new STA server. Click OK to all the fields, Save the NetScaler settings, then reopen the virtual server > Published Applications windows to verify the STA is now functional.

Q5 Why are we getting the 1030 on occasion but not every time?
A. Although each VDI-in-a-Box server in a grid will sync the time, on occasion it may drift farther than expected, causing the STA token to be invalid if the time is more than 60 seconds off. Simply log into the VDI-in-a-Box web console and go to the Admin tab. Click the Grid Time open and save it—this will force synchronization across the grid. To prevent the time from drifting more you can also just go to the Advanced Properties tab and use an NTP server for the entire grid. This will set a NTP server for the hypervisor host to use, which will ensure the VDI-in-a-Box Grid Time is synchronized.

Q6 Why won’t the VDI-in-a-Box web interface appear (page timeout or error code)?
A1. Log into the NetScaler web console, go to the Access Gateway Virtual Servers section, and open the Virtual Server created for VDI-in-a-Box remote access. Open the Policies tab and open the Session Policy you created. Modify the Session Profile and go to the Published Applications tab. Ensure the Web Interface Address field starts with https and has the VDI-in-a-Box Grid-wide Virtual IP.
A2. Make sure that SmartAccess option is not enabled for the Access Gateway Virtual Server. You must change to Basic mode. Once changed, save the settings, restart the web browser and attempt to view the VDI-in-a-Box login page through the Access Gateway.

Q7 Why are users prompted to type credentials twice when using a web browser?
A. VDI-in-a-Box 5.1 and earlier does not support for pass-through authentication from the Access Gateway for Single Sign-On (SSO). Enabled authentication on the Access Gateway prevents unauthorized users from access the VDI-in-a-Box resources over the Internet, as well as preventing various types of attacks (DoS). We plan to implement SSO support in a future release for web interface users. SSO is currently supported by PNAgent. Just add the VDI-in-a-Box account to your Citrix Receiver app (both computers and mobile devices).

Q8 Can I use SmartAccess, Full VPN, or Clientless VPN with VDI-in-a-Box?
A. At this time VDI-in-a-Box only supports Access Gateway in ICA Proxy mode with Basic mode enabled.
Q9 Can I use the NetScaler Load Balancing feature instead of the VDI-in-a-Box Grid-wide Virtual IP?

A. Yes this is supported and possible but not described in this document. Refer to the Configure NetScaler Access Gateway with VDI-in-a-Box 5.0 document for instructions on configuring Load Balancing.