

Configuring Secure64 Support

Configuring Secure64 Support

- Step 1: Create an nsd.conf file under the root directory / of your S64 Auth server
- Step 2: Make a directory for 6connect ProVision to push zone files to on the Secure64 DNS Server
- Step 3: Setup and Configure 6connect ProVision for your Secure64 DNS Server
 - Server Settings
 - 1) Set Server Common Settings
 - 2) Set Server Specific Settings
 - 3) Set DNS Group Settings for Server
 - 4) Save Changes
- Step 4: Associate zones to your Secure64 DNS Server(s)
- Step 5: Push Zones to Secure64 Server(s)
- Step 6: Verify DNS Zone push on Secure64 Server(s)
- Step 7: Validate Zone data in Your Infrastructure



A note on Ports

6connect uses port 22 to communicate with Secure64 infrastructure - please ensure that this is addressed in any ACLs/firewalls

The initial setup of the Secure64 Authoritative server is as follows:

Step 1: Create an nsd.conf file under the root directory / of your S64 Auth server



DO THIS

Make sure to add the line include: 6connect_nsd.conf to the nsd.conf file

Output/Input

```
[authdnsadmin@Secure64DNS]# cat nsd.conf
server:
ip-address: 50.198.192.141

axfr-logfile: /axfr_log/axfr.log
axfr-logfile-flush-count: 1
axfr-logfile-max-size: 100000
axfr-logfile-max-size: 10

request-logfile: /request_log/request.log
request-logfile-flush-count: 10
request-logfile-max-size: 1000000
request-logfile-max-files: 10

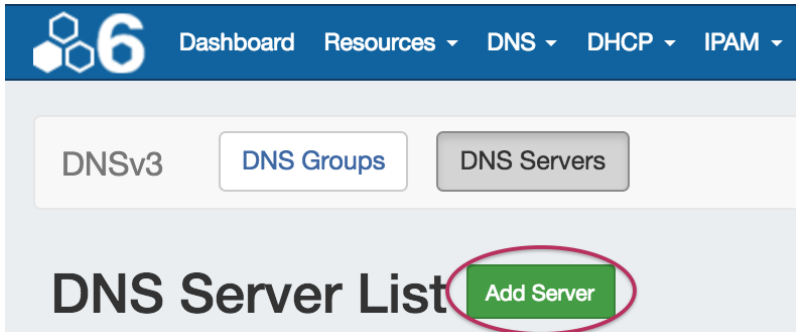
include: 6connect_nsd.conf
```

Step 2: Make a directory for 6connect ProVision to push zone files to on the Secure64 DNS Server


```
[authdnsadmin@Secure64DNS]# mkdir test12
[authdnsadmin@Secure64DNS]# ls
/:
322 2013-08-19 06:07:42 nsd.conf
<DIR> 1024 2013-08-16 17:30:12 test12
```

Step 3: Setup and Configure 6connect ProVision for your Secure64 DNS Server

To create a new server, start from the [DNS](#) Tab, select the **DNS Servers** sub menu. Then, click the "Add Server" button next to "DNS Server List".



This will open the "Server Settings" page.

Server Settings

1) Set Server Common Settings

In the "Common Settings" section of Server Settings, enter the new server's Display Name (the name that will appear on the ProVision interface), the FQDN / IP, server type, DNS service type, and desired parent Resource (may be left at the default Top Level Resource). For Secure64 servers, ensure that DNS Service is set to "Secure64 Authority", "Secure64 x86 Authority", "Secure64 KNOT Authority", or "Secure64 Cache".

The screenshot shows the 'Common Settings' form for a new DNS server. The form has several fields with red arrows pointing to them: 'Display Name' (with a placeholder 'Enter Display Name'), 'FQDN or IP' (with a placeholder 'ex: ns1.dns.6connect.net or 216.239.32.10'), 'Server Type' (set to 'Master'), 'DNS Service' (set to 'Secure64 Authority'), and 'Parent Resource' (set to 'TLR'). Each field has a dropdown arrow on the right. Below the 'Parent Resource' field, there is a note: 'The new server resource will be a child of the Parent Resource.'

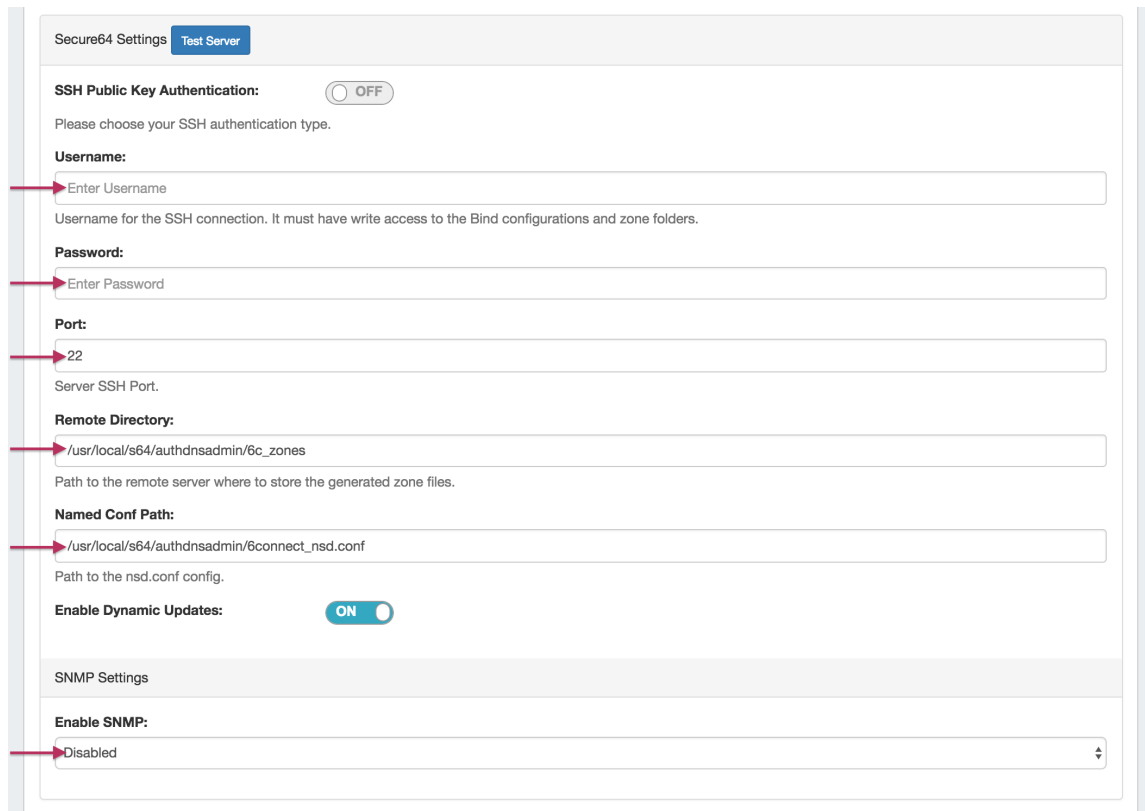
2) Set Server Specific Settings

The next section is entering server service-type specific settings. The options visible in this section will depend on the "DNS Service" type chosen under "Common Settings".

Here, we see the fields for Secure64 server settings.

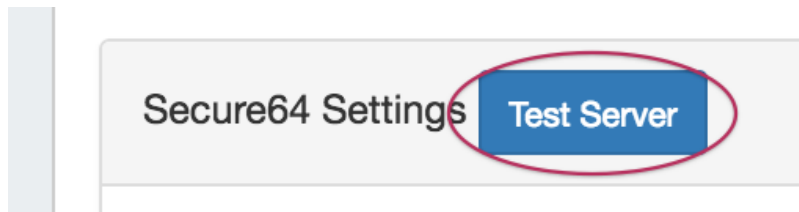
Enter the server Username, Password, Port, Remote Directory, Named Conf. Path, and whether to enable SNMP.

For SSH Public Key Authentication and Dynamic Option updates, click on the ON / OFF toggle to select "ON" or "OFF" for each as needed.

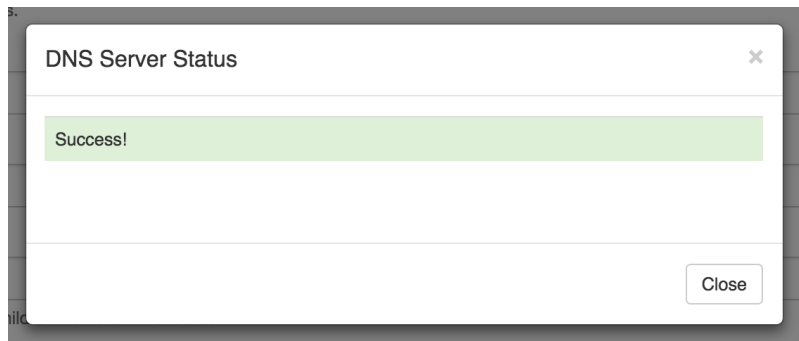


The screenshot shows the 'Secure64 Settings' form. At the top, there is a 'Test Server' button. Below it, the 'SSH Public Key Authentication' section has a toggle switch set to 'OFF'. A text prompt says 'Please choose your SSH authentication type.' The 'Username:' field has a red arrow pointing to it with the text 'Enter Username'. Below it, a note says 'Username for the SSH connection. It must have write access to the Bind configurations and zone folders.' The 'Password:' field has a red arrow pointing to it with the text 'Enter Password'. The 'Port:' field has a red arrow pointing to it with the text '22'. Below it, a note says 'Server SSH Port.' The 'Remote Directory:' field has a red arrow pointing to it with the text '/usr/local/s64/authdnsadmin/6c_zones'. Below it, a note says 'Path to the remote server where to store the generated zone files.' The 'Named Conf Path:' field has a red arrow pointing to it with the text '/usr/local/s64/authdnsadmin/6connect_nsd.conf'. Below it, a note says 'Path to the nsd.conf config.' The 'Enable Dynamic Updates:' section has a toggle switch set to 'ON'. Below this is the 'SNMP Settings' section, which has a dropdown menu for 'Enable SNMP:' with 'Disabled' selected. A red arrow points to the dropdown with the text 'Disabled'.

After entering the server-specific settings in this section, you can click the "Test Server" button at the top of the section to test the server connection and authentication.



A window will pop up showing a success or failure response.



3) Set DNS Group Settings for Server

In the last section, select whether to enable support for exporting DNS Groups as Views (click to toggle ON / OFF), and select a default Group, if desired, to be associated with the server. Zones assigned to the selected Group will automatically be attached to the server.

DNS Group Settings

Export Groups as Views: ☐ OFF
 Check this option if you want to enable the support of different DNS Groups to be exported as Views.

Attach to Group:
 No Default Group

If you select a default DNS group to your server, the zones assigned to this group will be automatically attached to the server.

Save changes

4) Save Changes

Save your changes when done! Just click the "Save Changes" button at the bottom right of the page.

DNS Group Settings

Export Groups as Views: ☐ OFF
 Check this option if you want to enable the support of different DNS Groups to be exported as Views.

Attach to Group:
 DNS Group 1

If you select a default DNS group to your server, the zones assigned to this group will be automatically attached to the server.

Save changes

Step 4: Associate zones to your Secure64 DNS Server(s)

If a default Group was selected while setting up the S64 server, then any zones in that Group will automatically be associated with the server.

Zones may be manually added, moved, or imported into the Group - see [Working with DNS Zones](#) and [Working with DNS Groups](#) for details on associating zones with Groups.

If zones are to be imported, a DNS Group may be selected during the import process to associate with the zones.

New Import

The DNS Import accepts an archive file of zones (ZIP or TAR) in both flat and hierarchical formats. You may also submit a CSV file mapping zone names to customer ids and DNS servers. Please make sure the archive file has an appropriate file extension, and that all files are encoded in UTF-8.

DNS Group: DNS Group 1

Job Name:

Description:

Configuration File:
 Choose File No file chosen
 Required: a configuration file in BIND or NSD format.

Archive File:
 Choose File No file chosen
 Required: a ZIP or TAR of your zones.

CSV File:
 Choose File No file chosen
 Optional: a CSV file mapping zones to customers and DNS Servers.

Start Import

Select the group specified as the default S64 server Group, then import the zones as described in the [Import DNS Zones](#) documentation.

Step 5: Push Zones to Secure64 Server(s)

Navigate back to the [DNS](#) tab, and select the "DNS Servers" tab.

Locate the Secure64 server in the DNS Servers list, and then click the "Push" button under "Actions" at the end of the row.

6c S64 Server1	SECURE64	master	Delete Push
----------------	----------	--------	-------------

Step 6: Verify DNS Zone push on Secure64 Server(s)

The result of the Push can be checked/verified by checking the Secure64 server as follows:



Verifying Zone pushes

```
ssh to 50.198.192.141
Login using the designated login account and password
Enable cachednsadmin
ls
```

Now, verify that the "788 2013-08-21 12:35:04" 6connect_nsd.conf file now exists.

```
[authdnsadmin@eval138.secure64.com]# ls
/:
6728 2013-08-13 00:15:30 nsd.conf
8416071 2013-08-21 12:35:07 nsd.db
788 2013-08-21 12:35:04 6connect_nsd.conf
<DIR> 1024 2013-08-21 12:34:50 test12
```

You can verify the Push contents by doing a cat of the 6connect_nsd.conf



```
[authdnsadmin@Secure64DNS]# cat 6connect_nsd.conf
```

AutoGenerated by 6connect ProVision. Do not manually edit.

zone:

name: atestzone.com

zonefile: /test12/6connectGeneric/m/atestzone.com.zone

zone:

name: Testzone2.com

zonefile: /test12/6connectGeneric/m/Testzone2.com.zone

In the example above, two Zones have transferred.

To look at the contents of each zone you can cd to the proper directory /test12/6connectGeneric and find the zone files in an alphabetical directory structure as follows:


```
i [authdnsadmin@Secure64DNS]# cd 6connectGeneric

[authdnsadmin@Secure64DNS]# cd test12

changed to test12
[authdnsadmin@Secure64DNS]# ls
/test12/:
DIR 1024 2013-08-16 19:43:21 6connectGeneric
[authdnsadmin@Secure64DNS]# cd 6connectGeneric
changed to 6connectGeneric
[authdnsadmin@Secure64DNS]# ls
/test12/6connectGeneric/:
DIR 1024 2013-08-16 17:30:13 e
DIR 1024 2013-08-16 17:30:16 m
DIR 1024 2013-08-16 18:49:21 d
DIR 1024 2013-08-16 19:43:23 s
[authdnsadmin@Secure64DNS]# cd m
changed to m
[authdnsadmin@Secure64DNS]# ls
/test12/6connectGeneric/m/:
[authdnsadmin@eval138.secure64.com]# ls
5192 2013-08-21 15:35:01 atestzone.com.zone
6758 2013-08-21 15:35:02 Testzone2.com.zone
[authdnsadmin@Secure64DNS]#
```

Step 7: Validate Zone data in Your Infrastructure

Finally, do a **dig** of the zones to verify the DNS configuration has been successfully deployed.

```
i Using dig to validate your Secure64 Server installation

[authdnsadmin@eval138.secure64.com]# dig @50.198.192.141 atestzone.com
; DiG SourceT 3.x @50.198.192.141 atestzone.com
;; Got answer:
;; HEADER opcode: QUERY, status: NOERROR, id: 59591
;; flags: qr aa rd: QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;atestzone.com. IN A
;; AUTHORITY SECTION:
atestzone.com. 3600 IN SOA ns1.dns.6connect.net. hostmaster.6connect.net. (2013082102 10800 3600 604800 38400 )
[authdnsadmin@eval138.secure64.com]#
```

For any questions regarding the integration of Secure64 products into 6connect ProVision, please email 6connect at support@6connect.com, or Secure64 at support@secure64.com