

# 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 ProVision to push zone files to on the Secure64 DNS Server
- Step 3: Setup and Configure 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

### Additional Information

#### A note on Ports

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

ProVision also uses port 53 to do zone checks if the DNS Module is enabled and in use. Please ensure that your Secure64 infrastructure is configured to accept DNS lookups from the ProVision server

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

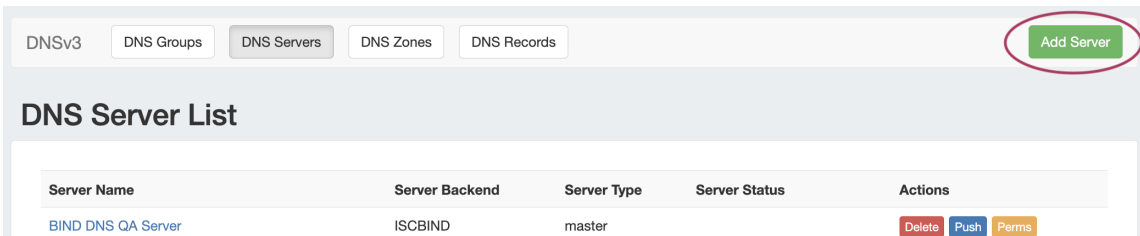
include: 6connect_nsd.conf
```

## Step 2: Make a directory for 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 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".



The screenshot shows the 'DNS Server List' interface. At the top, there are tabs for 'DNSv3', 'DNS Groups', 'DNS Servers', 'DNS Zones', and 'DNS Records'. The 'DNS Servers' tab is selected. In the top right corner, there is a green 'Add Server' button, which is circled in red. Below the tabs, the title 'DNS Server List' is displayed. Underneath, there is a table with the following columns: 'Server Name', 'Server Backend', 'Server Type', 'Server Status', and 'Actions'. The table contains one entry: 'BIND DNS QA Server' with backend 'ISCBIND' and type 'master'. The 'Actions' column for this entry has three buttons: 'Delete' (red), 'Push' (blue), and 'Perms' (orange).

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".

Common Settings

**Display Name:**

Enter Display Name

This is the server name that will appear in the DNS interface.

**FQDN or IP:**

ex: ns1.dns.6connect.com or 216.239.32.10

The IP address that ProVision will use to connect to this server.

**DNS Port:**

default: 53

The port will be used for DDNS and DNS Queries to the server.

**Server Type:**

Master

**Export Zones:** ☐ OFF

**DNS Service:**

Secure64 Authority

**Parent Resource:**

TLR

The new server resource will be a child of the Parent Resource.

**Enable Records Check:** ☐ OFF

ProVision is checking if the DNS responds with a proper values to the zone records. In order record monitoring to work properly, you must enter a proper NameServer as "FQDN or IP" field.

**Enable TSIG Key for transfers:** ☐ OFF

If enabled, the provided TSIG key will be added to the ACL config of the related DNS Servers.

## 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 enabled 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.

Secure64 Settings

**SSH Public Key Authentication:** ☐ OFF

Please choose your SSH authentication type.

**Username:**

Username for the SSH connection. It must have write access to the Bind configurations and zone folders.

**Password:**

**Port:**

Server SSH Port.

**SSH Route:**

Use ssh routes in order to define a chain from ssh jump hosts.

**Remote Directory:**

Path to the remote server where to store the generated zone files.

**Named Conf Path:**

Path to the nsd.conf config.

**Public IP Address:**

The public-facing IP address for this server used in writing server configs. If omitted, the 'FQDN or IP' field will be used.

**Enable Dynamic Updates:** ☒ ON

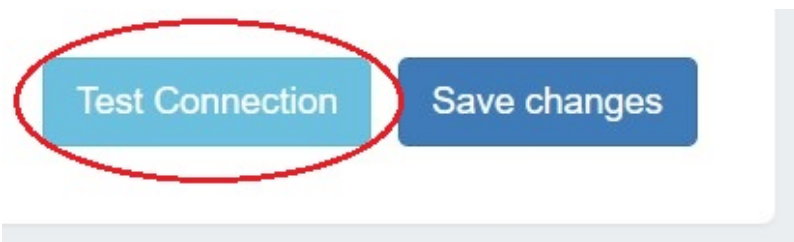
**Enable Configuration Rollback:** ☐ OFF

If the Configuration Rollback is enabled on push, ProVision will move the current configuration and zone files to a different files with prefix \_backup. In case of failure you can restore the previous configuration with prefix \_backup.

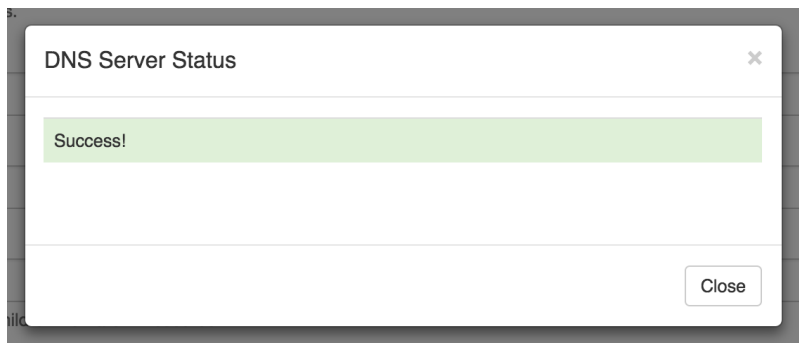
SNMP Settings

**Enable SNMP:**

After entering the server-specific settings in this section, you can click the "Test Connection" button at the bottom right of the page 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

Multiple Groups Support:

☐ OFF

Check this option if you want to enable the support of different DNS Groups to be exported as Views. **Danger !** In case the server doesn't support Views you must take care to not have duplicated zone names in the groups !

Export Groups as Views:

☐ OFF

If this option is checked the Groups will be exported as Views on push. (It works only on servers that support Views like ISC BIND)!

Attach to Group:

Example Group

▼

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

### 4) Save Changes

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

DNS Group Settings

Multiple Groups Support:

☐ OFF

Check this option if you want to enable the support of different DNS Groups to be exported as Views. **Danger !** In case the server doesn't support Views you must take care to not have duplicated zone names in the groups !

Export Groups as Views:

☐ OFF

If this option is checked the Groups will be exported as Views on push. (It works only on servers that support Views like ISC BIND)!

Attach to Group:

Example Group

▼

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

Test Connection

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.

DNS Zone Import

Clear

Step 1: 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:

Example Group

Job Name:

Sample Zone Import

Description:

Example

Configuration File:

Choose File

No file chosen

Optional: a configuration file in BIND or NSD format. If it is not provided the ZIP or TAR must be a flat archive from zone files.

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.

## OTHER Record Types

When working with DNS Zones and Records, additional record types may be manually added by selecting "Other" when adding a new record.

S64 DNS users can use record type "Other" to add "SYNTH" or "TYPE65464" type records similar to the format below:

```
$ORIGIN 30 IN TYPE65464 ${p4} PTR ${a4}.pool.example.com.
$ORIGIN 600 IN TYPE65464 ${a4} A ${a4}
$ORIGIN TYPE65464 ${p6} PTR user${a6}.my.example.com.
$ORIGIN 5 IN SYNTH user${a6} AAAA ${a6}
$ORIGIN IN SYNTH nptr-${u} NAPTR 10 20 "A" "" "" srv-${u}
$ORIGIN IN SYNTH srv-${u} SRV 10 20 1234 srv-addr-${u}
```

However, arbitrary / other record types are unable to be validated, so use with care!

## 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.

ANewServer	ISCBIND	master	<div> <div>Delete</div> <div>Push</div> <div>Perms</div> </div>
------------	---------	--------	---

## 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 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:

```
[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.

### 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 ProVision, please email 6connect at [support@6connect.com](mailto:support@6connect.com), or Secure64 at [support@secure64.com](mailto:support@secure64.com)

### Changing Secure64 Server IP addresses

When you setup ProVision to communicate via SSH to a Secure64 server, a key/fingerprint is saved to the local hosts file. If you modify the IP address, but do not clear out the hosts file, then ProVision will think this is an attack and prevent communication with the Secure64 server.

To rectify this issue, you may need to reset the host file so that a new SSH host key can be added for the IP address. To do this manually, please follow the following steps:

- 1) The admin needs to login to the ProVision server via SSH/CLI
- 2) Open the file "known" in the /tmp folder in your preferred editor (vi, etc.)
- 3) Delete the line in the file with the server IP/fingerprint
- 4) Save the changes and exit the editor

To verify the functionality - attempt to connect to the DNS Server(s) using the "Test Server" button from the ProVision GUI

If you have any issues, please contact 6connect support per your Support Agreement/Plan.

## Additional Information

For additional information on working in DNS, see the following sections:

- [Working with DNS Servers](#)
- [Configuring ISC BIND Support](#)
- [Configuring PowerDNS Support](#)
- [Configuring Split Horizon and Views](#)
- [Configuring DNSSEC](#)
- [Import DNS Zones](#)
- [DNS Tab](#)