Migrating from SEMS 3.x to 3.4.0

by Mike Ankeny - Senior Tech Support Engineer, Enterprise Encryption Support, Symantec Corporation  
This unofficial document is an outline of the process of migrating the server to version 3.4.0. All official Symantec documentation should be read before proceeding.

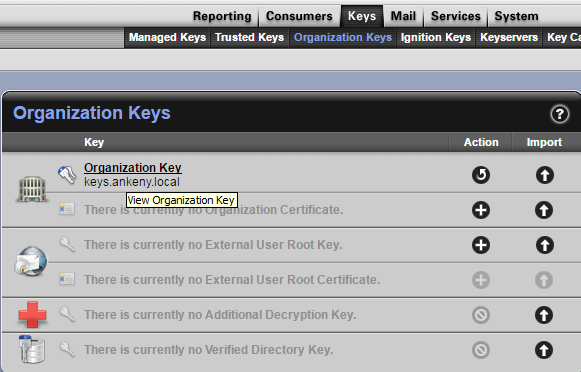
**NOTE: If your environment uses a hardware ignition key for the SEMS, you must contact support before proceeding with the migration process for additional steps.**

# Section 1: Backing up the organization key

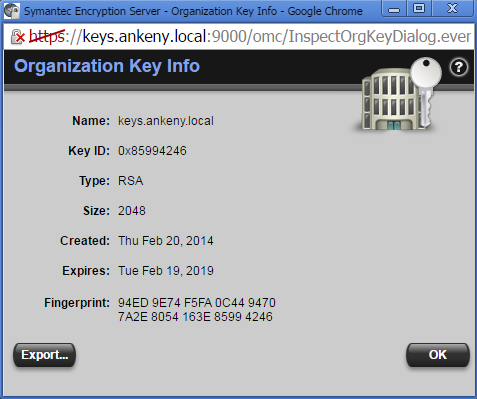
How to back up the Organization Key:  
<https://support.symantec.com/content/unifiedweb/en_US/article.HOWTO42046.html>

Due to the limitations of Tomcat/Apache, backup files over 2GB will need special precautions and procedures. You must have a copy of the Organization Key **without a passphrase assigned** if your backup is larger than 2GB. Here are the steps with screenshots:

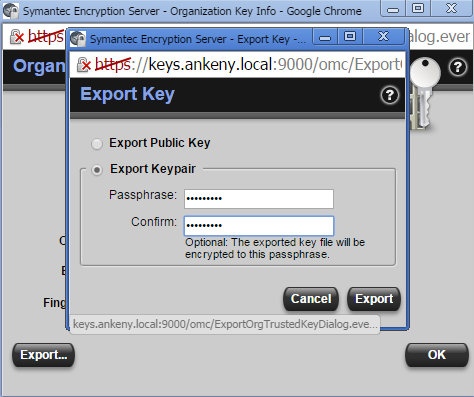
1. On the existing server, go to Keys, Organization Keys, and click where it says Organization Key



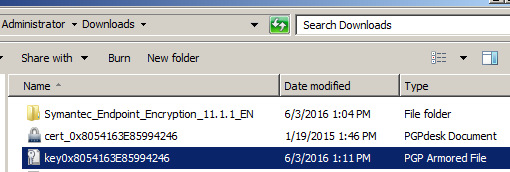
1. Select “Export”



1. Select “Export Keypair” and enter a password (unless you have a backup larger than 2GB, in that case do not enter a password). Then click “Export”.



NOTE: by default, your key will be saved in Downloads



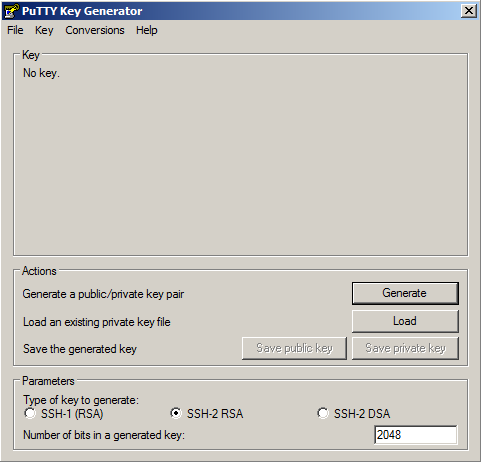
# Section 2: Obtaining a backup from the SEMS

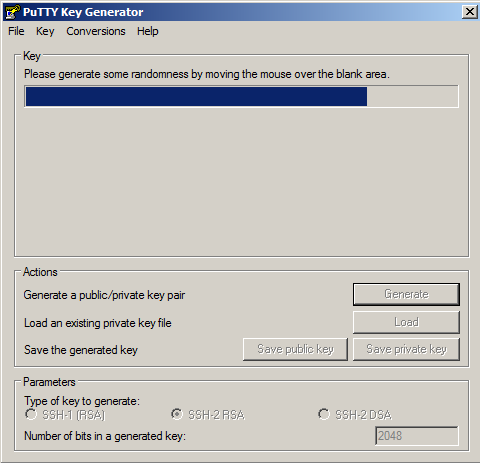
If you do not have the backups set to offload to another location, and they are stored on the SEMS locally, you will need to do the following:

## Set up SSH access:

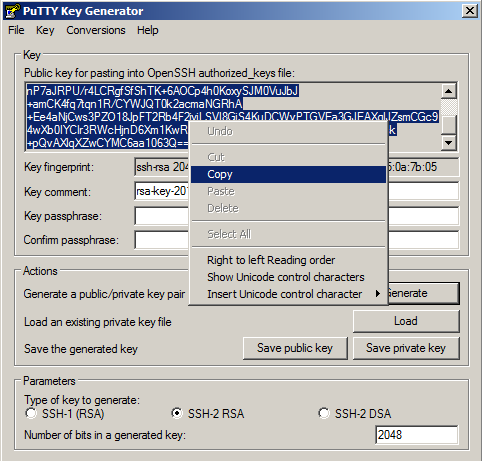
You will need Putty, Puttygen, and WinSCP (or similar applications). They can all be downloaded from <https://winscp.net/eng/download.php> but beware of ads. They are free tools, so get their revenue elsewhere. Putty and PuttyGen are lower down on the page.

1. Open PuttyGen. Click “Generate”, then move the mouse around in the grey area in the top section of the application to generate a key. Make sure 2048 is selected for the bitsize.

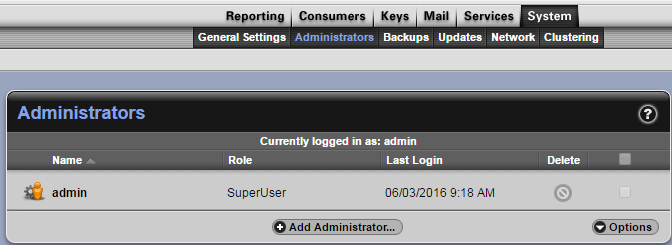




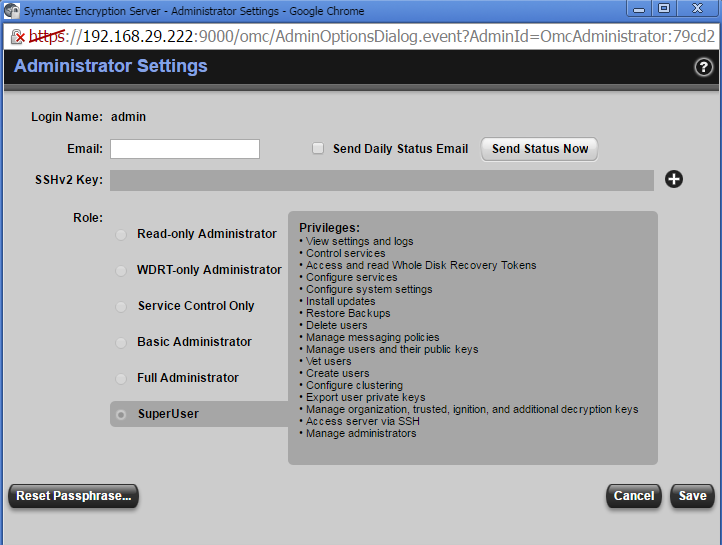
1. Select all of the text in the top section. Right-click and select “Copy”.



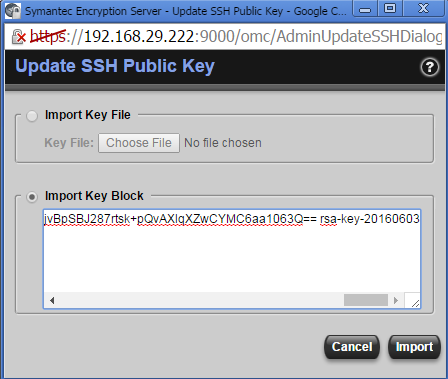
1. Log on to the SEMS. Select System>Administrators, and click the account to which you would like to add SSH access.



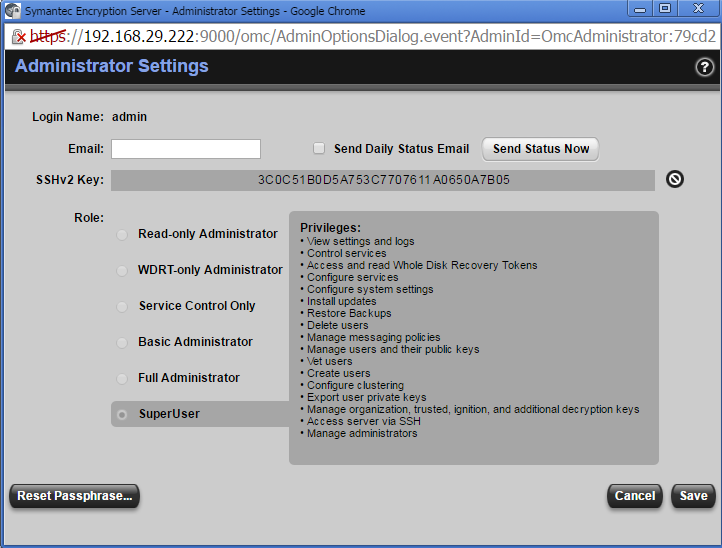
1. Click the “+” sign to the right of the SSHv2 Key box.



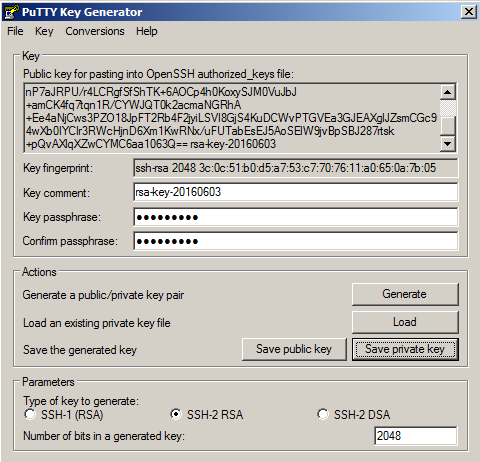
1. Select “Import Key Block”, then paste the key from PuttyGen and select “Import”.



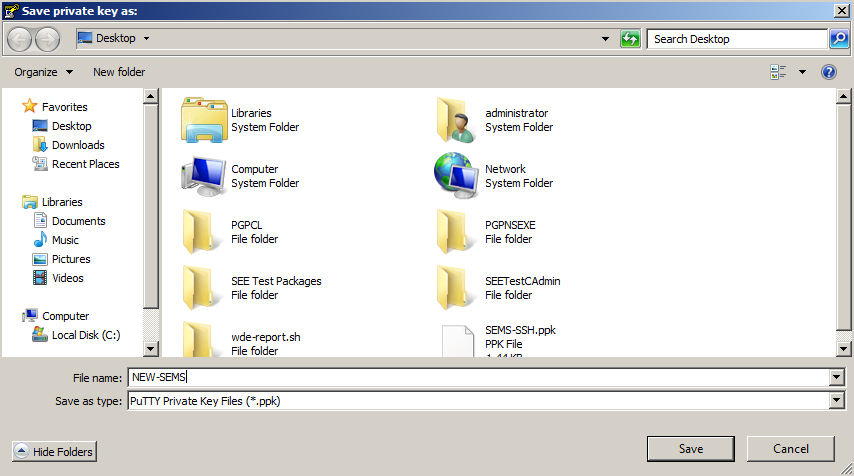
1. You will now see the SSHv2 Key box is populated. Select “Save”.



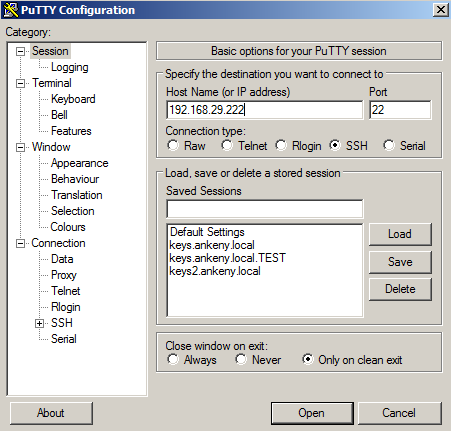
1. Return to PuttyGen. Assign a passphrase for the key, confirm the passphrase, and select “Save Private Key.



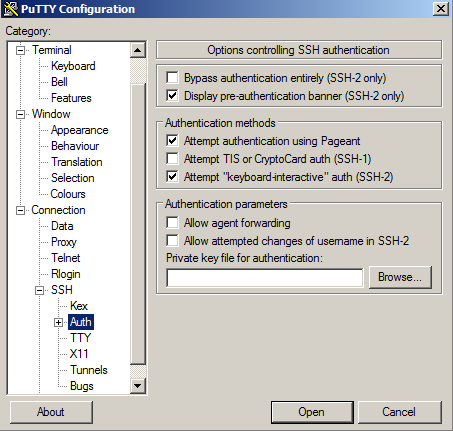
1. Save the key to a location you will have access to later in the process.



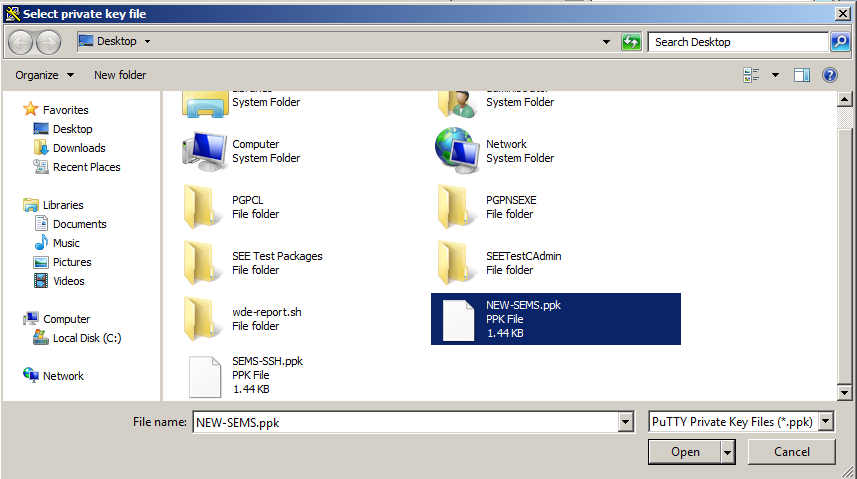
1. Open Putty. Enter the IP address of the current server.



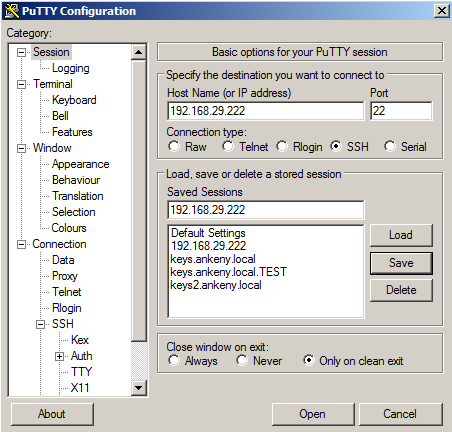
1. Expand ”SSH” on the left and click “Auth”. Under “Private key file for authentication”, select “Browse”.



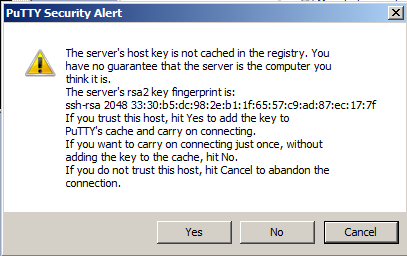
1. Select the key saved in step 7. Click “Open”.



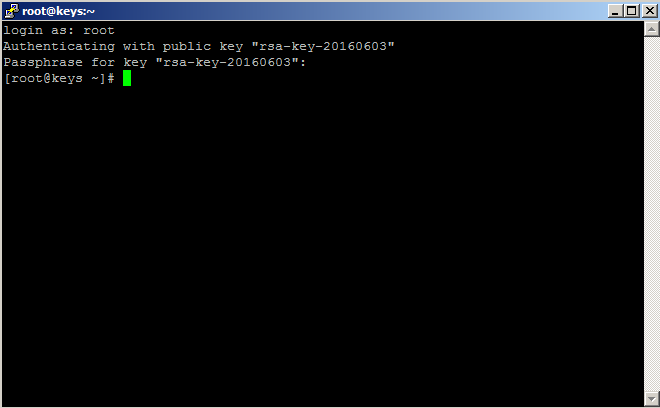
1. If you wish to save your session information, select “Session” from the left, give the session a name, and select “Save”. Then select “Open” to start the session.



1. You may get a warning similar to the following since the server’s host key is not cached yet by Putty. Click “Yes”.

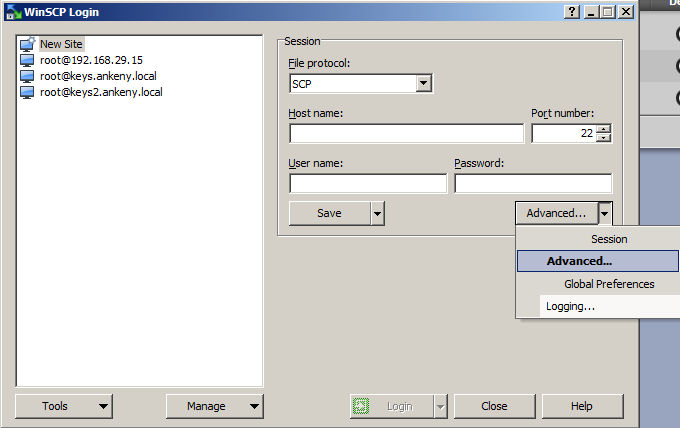


1. Enter “root” as the login. After entering that, you will be prompted for the key passphrase.

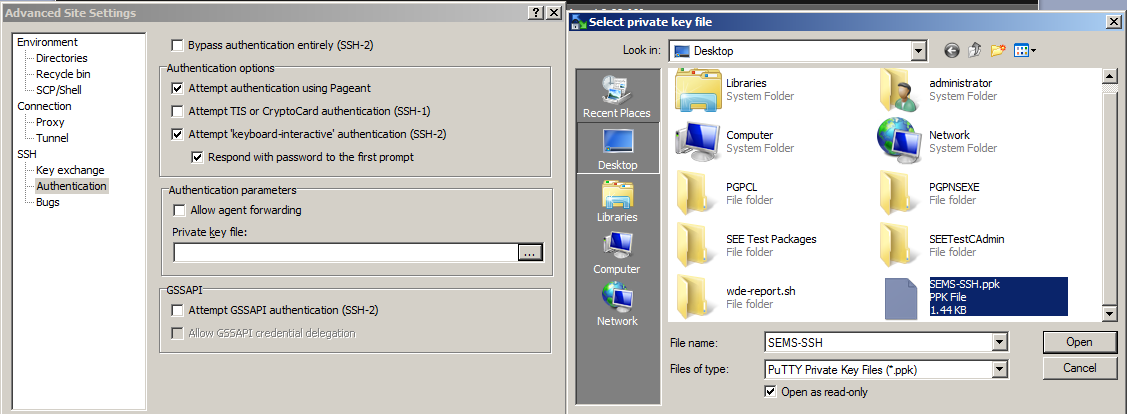


## Set up WinSCP for file transfers

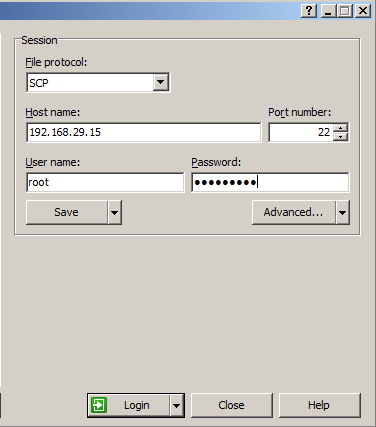
1. Select “SCP” as the file protocol. Then select “Advanced…”, and click “Advanced…”



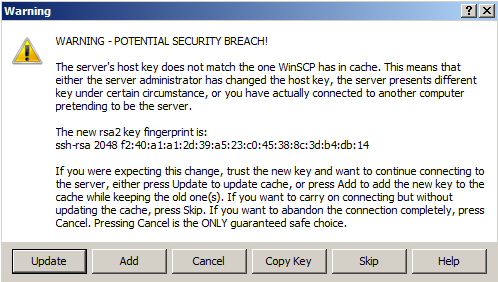
1. Select “Authentication” under “SSH”. Select the “…” button next to the Private Key File box, and locate the key you used for Putty. Select Open.

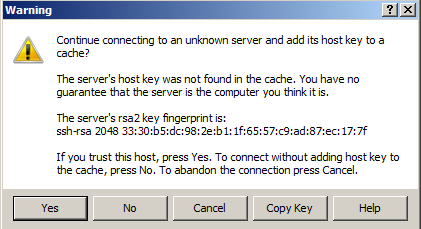


1. Enter the host name, and use “root” as the user name. You can enter the key passphrase here or you will be prompted for it when you log in. If desired, select “Save”, then “Login”.



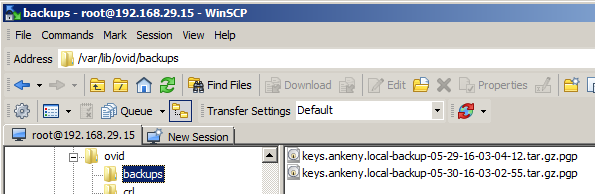
1. Similar to Putty, you will get a warning similar to one of the below examples. Select “Update” or “Yes”.



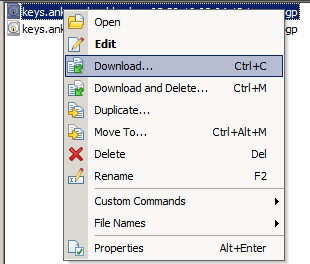


## Downloading the backup

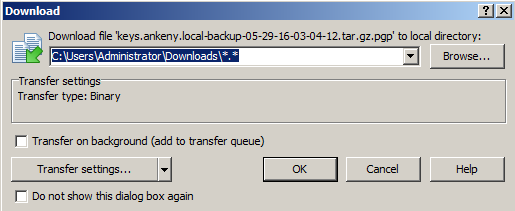
1. Navigate to /var/lib/ovid/backups.

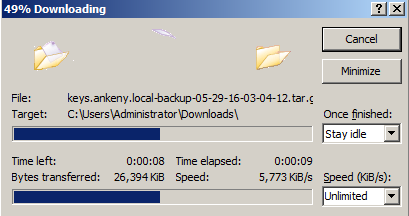


1. Right-click the desired backup, and select “Download”.



1. Select a save location for the backup. Click “OK”.



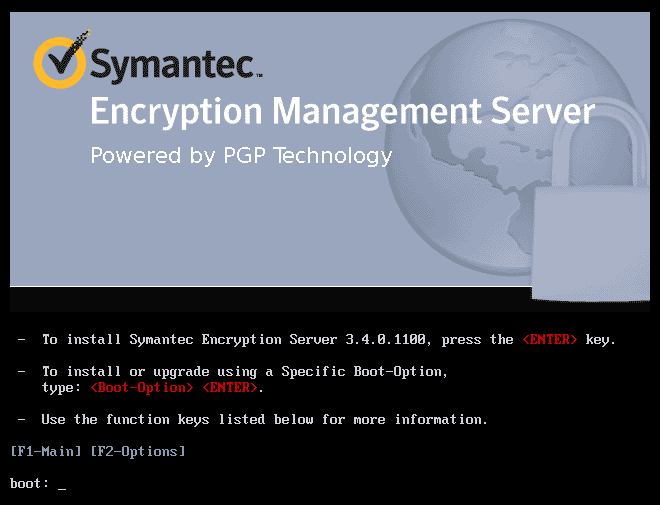


# Section 3: Installing the new server

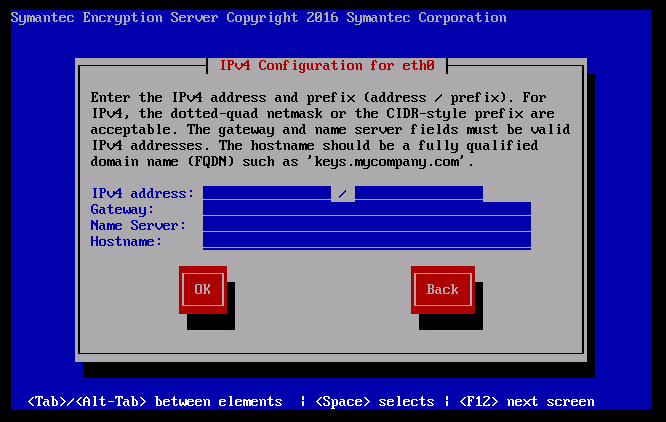
If your backup is less than 2GB in size, you can follow the directions here to finish the process:  
<https://www.symantec.com/connect/articles/how-migrate-pgp-universal-or-symantec-encryption-management-server>

If the backup is larger than 2GB, you will need to perform the following steps:

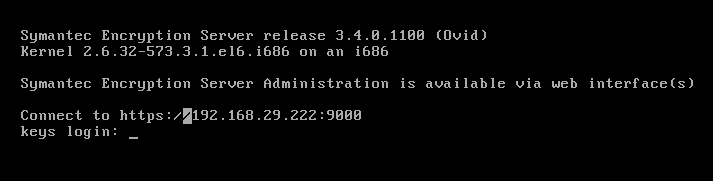
1. Insert the boot disc (or mount the ISO in a VM) for Symantec Encryption Management Server 3.4.0. Boot the system, and you should see the following screen. Press “Enter” if ready to proceed.



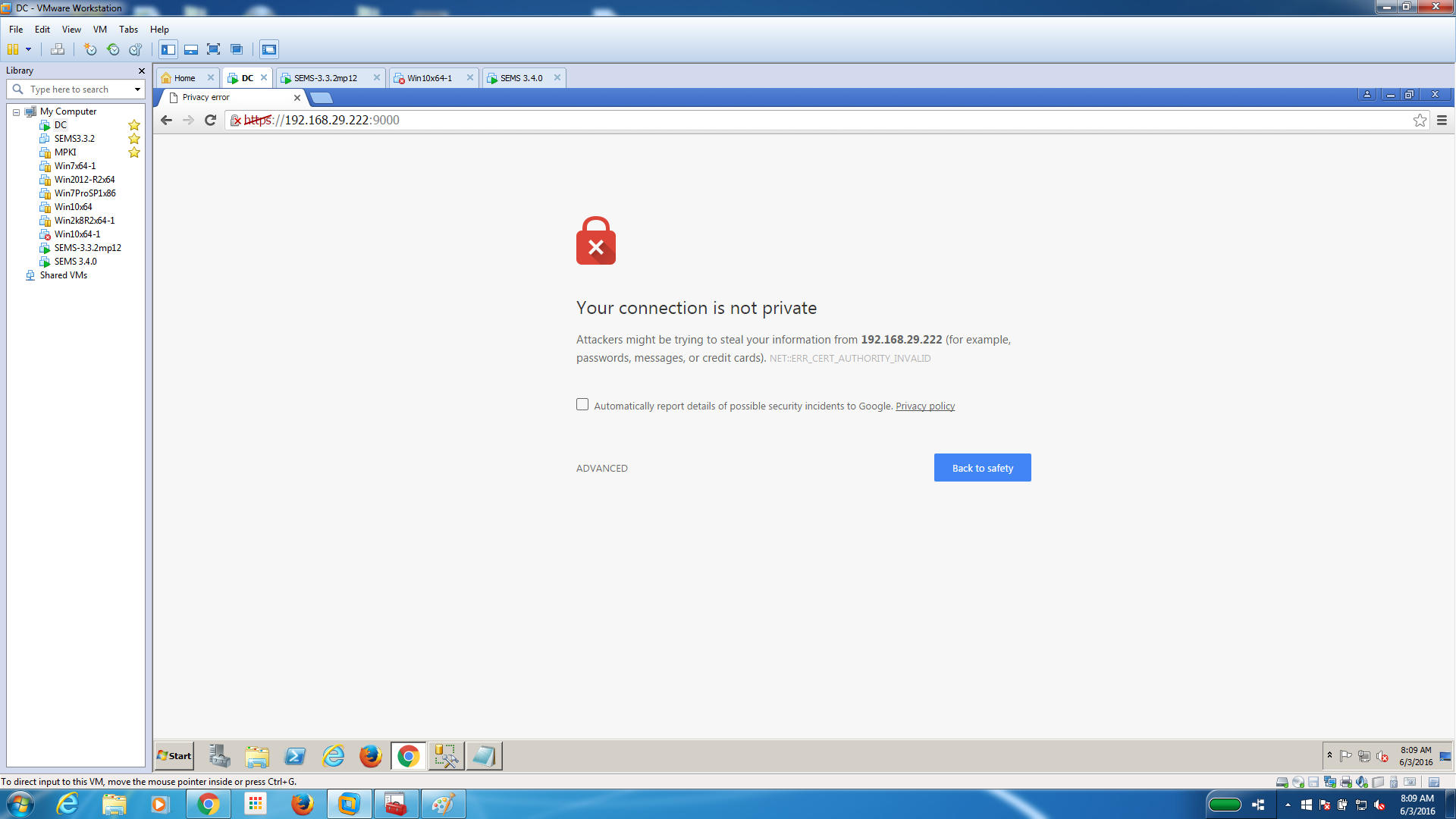
1. Enter the IPv4 address and netmask, Gateway, DNS Server, and Hostname you will be using temporarily for the install. The restore process will overwrite all of these settings. Select “OK”.



1. The rest of the initial installation will proceed automatically, and bring you to this prompt:



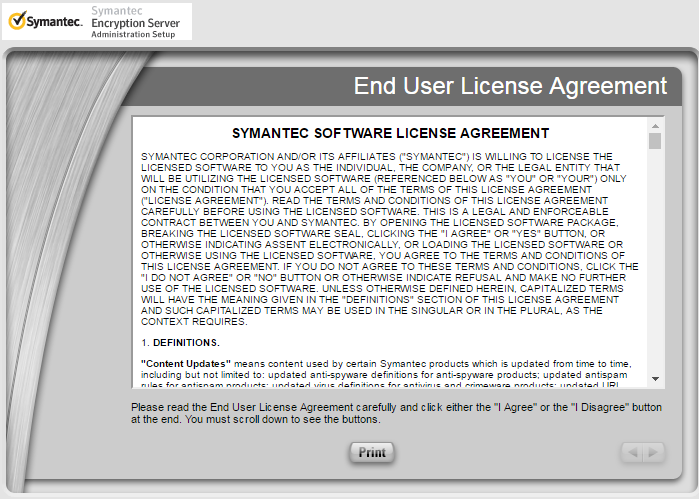
1. Access the new server in a web browser using the IP address you previously entered in step 2. You will most likely get a browser warning, but it should be safe to proceed.



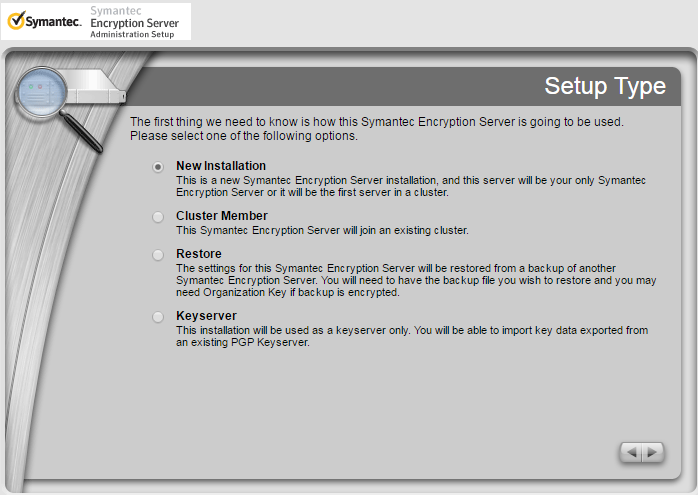
1. Click the arrow button to continue.



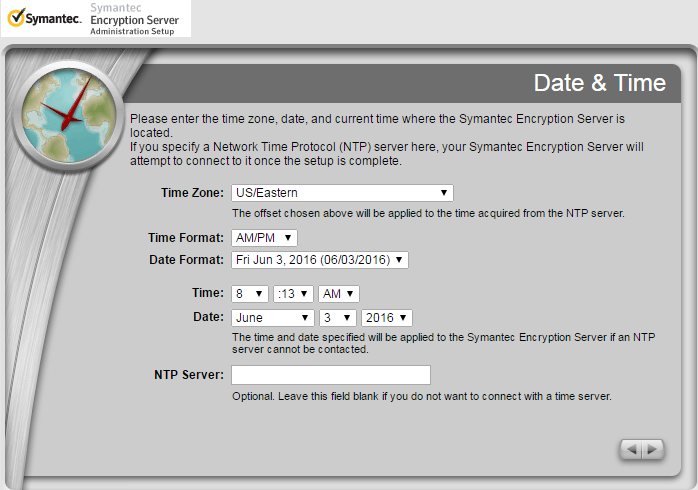
1. Read the license. When you reach the bottom, if you accept, press “I Accept”.



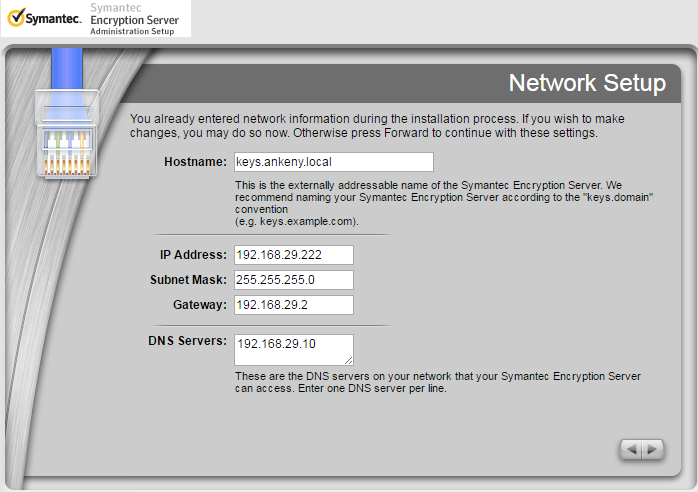
1. Select “New Installation” and click the arrow button to advance.



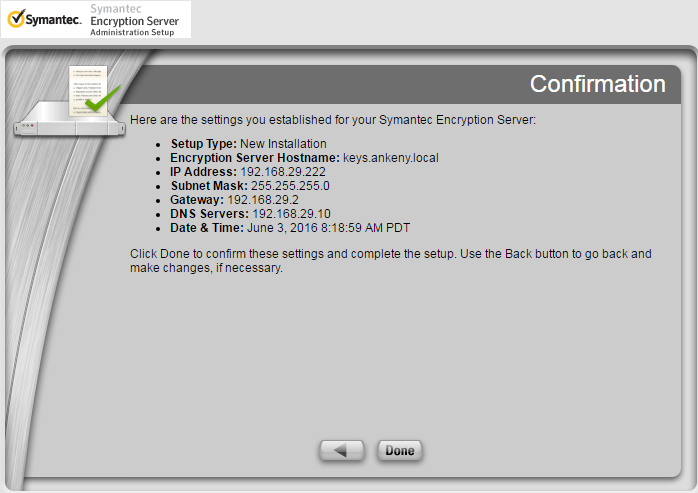
1. Set the date and time, then click the arrow button to continue.



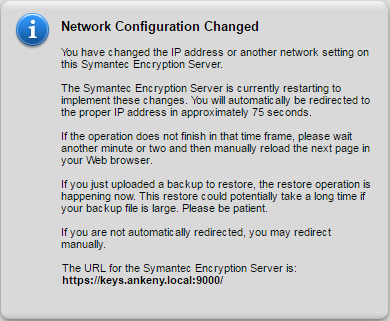
1. Confirm that the settings are correct, and click the arrow button to continue.



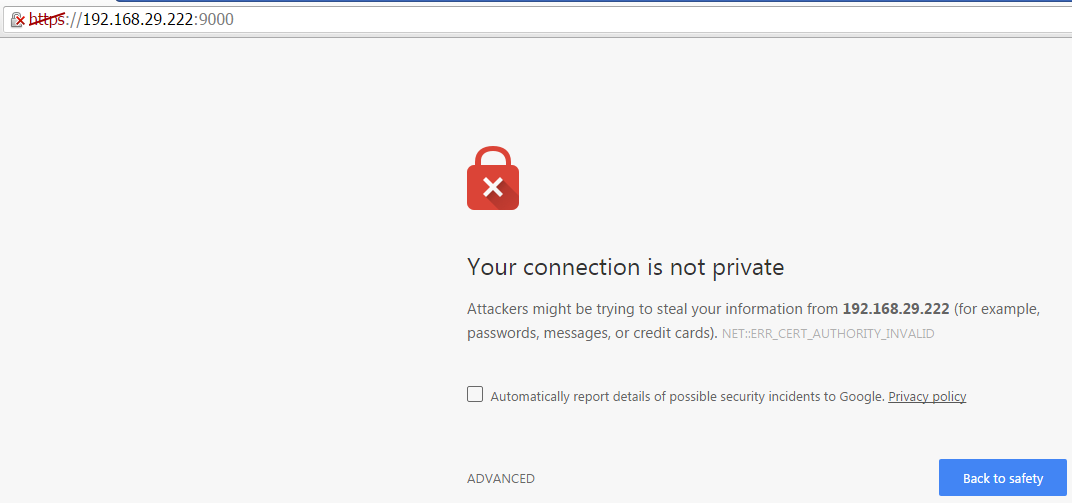
1. Select “Done”.



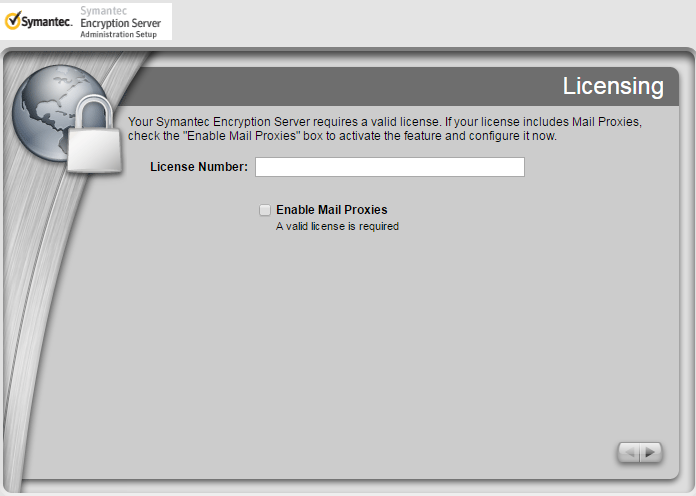
1. The system will restart to implement the changes for this part of the installation process. It will periodically refresh the page. If you did not create a temporary DNS entry, you will need to manually try by IP address.



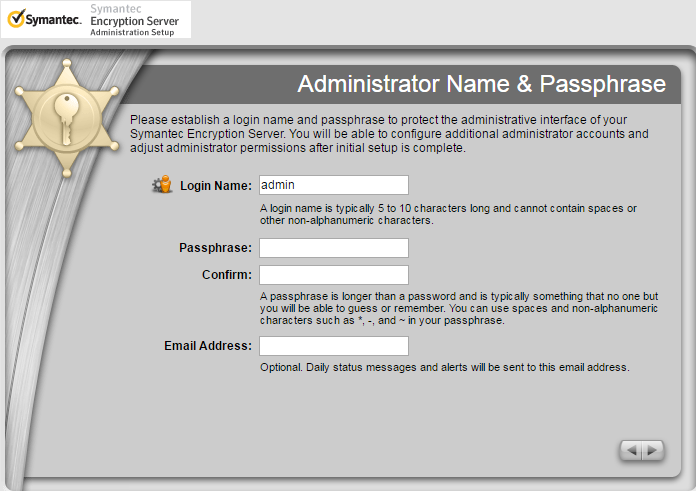
1. After the server comes back online, you will be given the certificate warning again. Proceed past it.



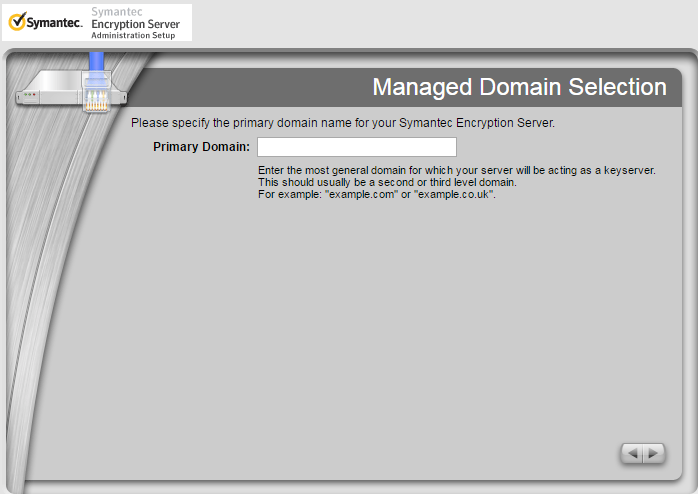
1. Enter your existing license number from your previous server into the new server. If you were issued a new license number, use that instead. Click the arrow button to continue.



1. Select a default username and passphrase for the admin account. This will be overwritten during the restore process. Click the arrow button to continue.



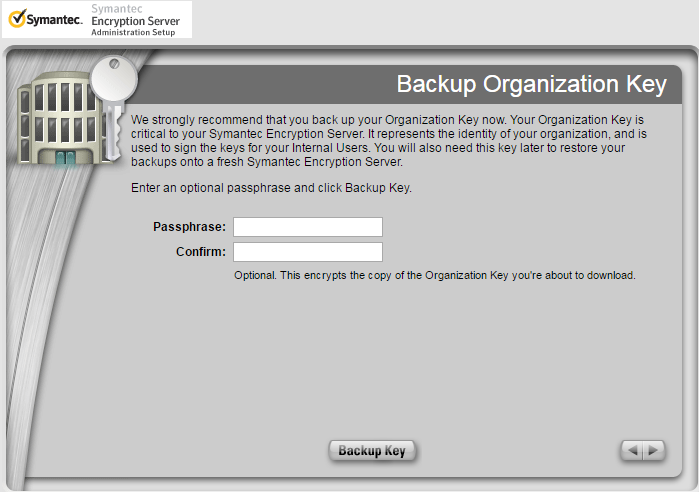
1. Enter the primary domain for the server, then click the arrow button to continue.



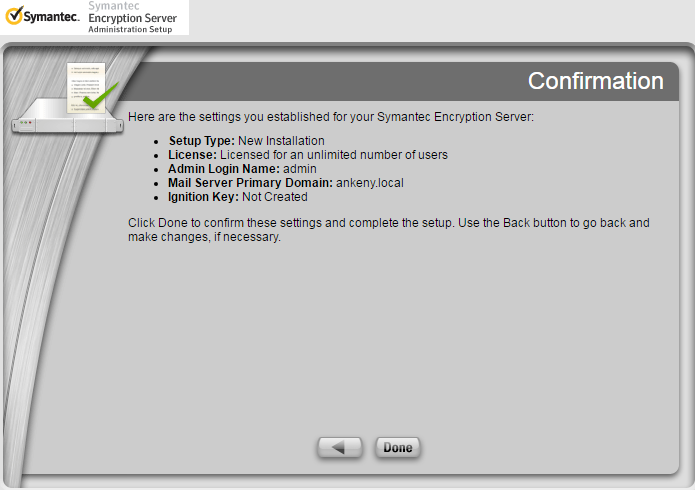
1. Since it will be overwritten anyway, I would recommend skipping the ignition key. Click “Skip”.



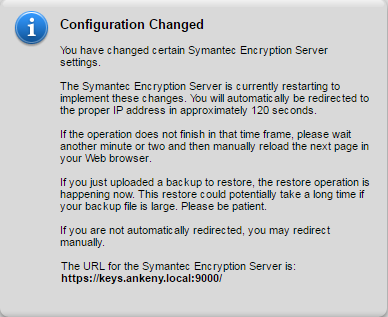
1. As it will be overwritten, I would recommend not backing this key up, but simply moving to the next page by pressing the arrow button.



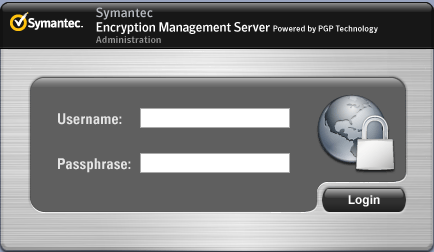
1. Select “Done”.



1. The server will restart again to complete the installation.



1. After the server restarts, you will again need to access it through the web portal using the temporary IP address.



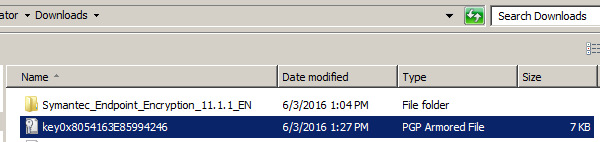
1. The following screen will appear. Click “Close”.

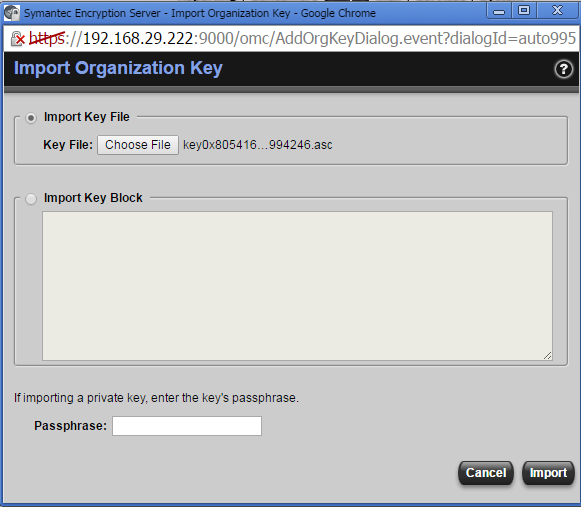


1. Select Keys>Organization Keys. Click the up arrow under “Import”.

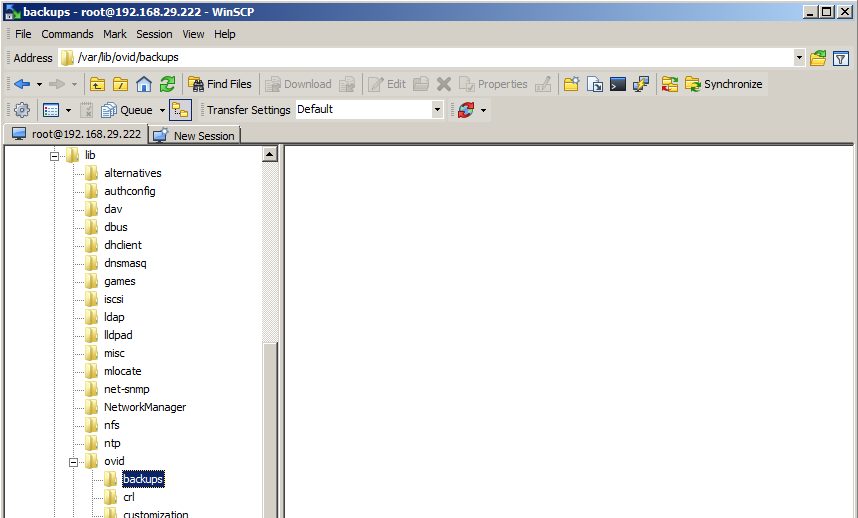


1. Click “Choose File”. Browse to the location of the saved keypair. Select your Organization Key backup, and select “Open”. Select “Import”.

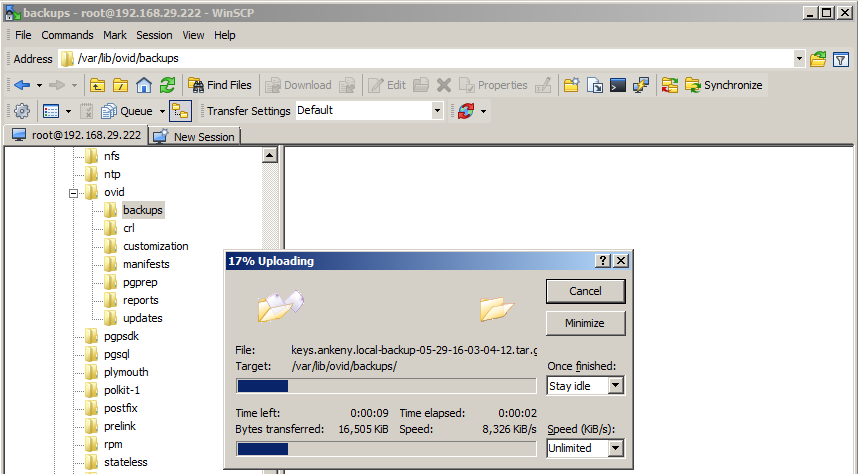


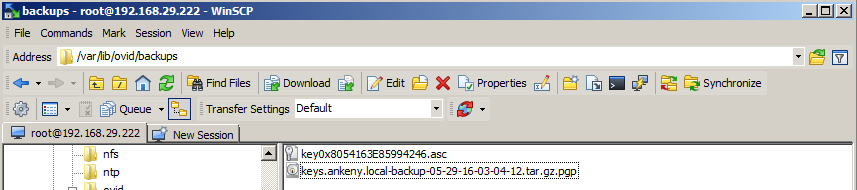


1. Set up SSH access and WinSCP access using steps from Section 2: A&B in this document. These keys will be overwritten on restore.
2. Once you have WinSCP set up for the new system, open a session. Navigate to /var/lib/ovid/backups

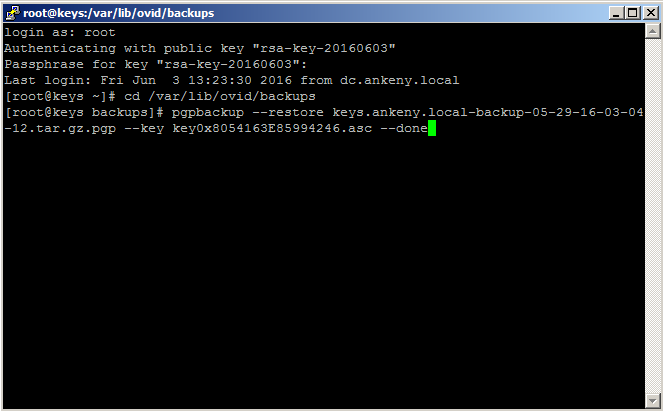


1. Upload your server backup and Organization Key backup into the Backups directory.

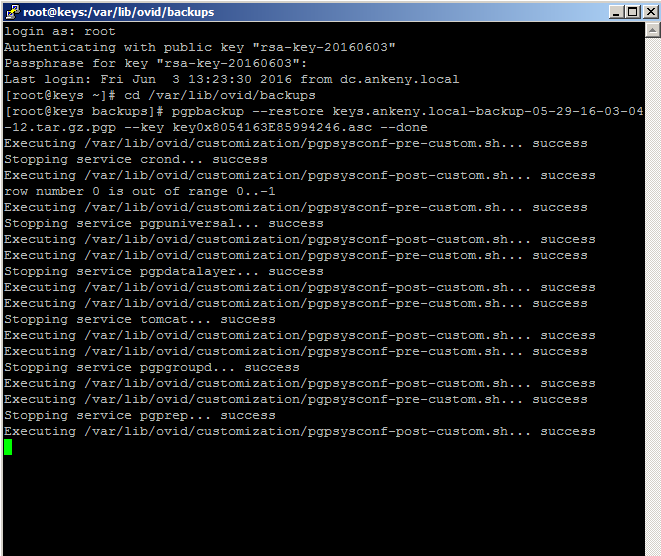


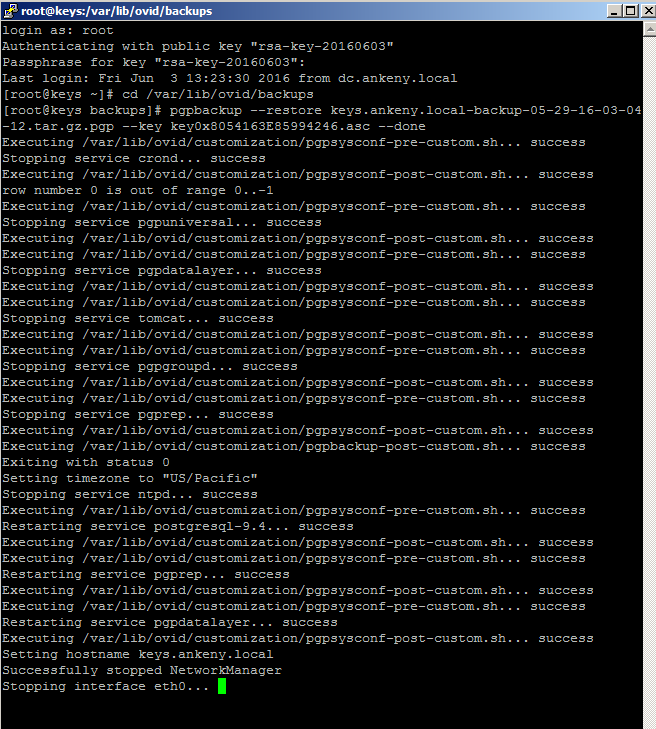


1. We next will need to open an SSH session with Putty on the new server. After establishing the session, we need to manually restore the backup using the following format command:  
   pgpbackup --restore *YourBackupName* --key *YourKeyID* --done  
     
   An example follows. You can hit the ‘tab’ key to autocomplete commands, so you don’t need to type everything out completely. In the following case, I typed:  
   pgpbackup --restore keys<tab> --key key0<tab> --done



1. The server will start processing the restore using the backup and copy of the Organization Key. Delete the copy of the key from ‘/var/lib/ovid/backups’ when finished. At a certain point after it changes the network interface, Putty will stop functioning. You should then ping the old server IP until it comes back up, then should be able to log in using the old credentials.





# Section 4: Verification

1. Verify that you are able to log in to the server through the Web Console.
2. Verify that you are able to log in to the server via SSH.
3. Verify that your users and user groups are present.
4. Verify users are able to check in.
5. Verify Web Email Protection clients can log in if applicable.
6. Verify backups are able to save in the specified location.

**If you encounter any issues after upgrade, contact technical support for assistance.**