

Silently installing Exceed TurboX Nodes

Silently installing Exceed TurboX Nodes

This section provides information about how to silently install Exceed TurboX Connection Nodes.

For more information, see the following topics:

- [Exceed TurboX Node silent installation on Linux and UNIX systems](#)
- [Exceed TurboX Node silent installation on Windows systems](#)

Exceed TurboX Node silent installation on Linux and UNIX systems

Exceed TurboX Node silent installation on Linux and UNIX systems

This section provides information about the Exceed TurboX Node silent installation on Linux and UNIX systems.

Note

The node silent installation requires `sudo` privileges.

To install a node silently, run the following command:

```
sudo bin/install -s fullpath/responsefile
```

The `-s` (silent) parameter requires the path to a response file. The `responsefile` contains responses to installation questions and has a specific format. A sample response file is available in the node tar package (`/conf/response.etxcn.template`). To specify install options for the node, edit the `response.etxcn.template` file in a text editor, then pass the path to the edited file when specifying the `-s` option.

You can configure the following properties in the node response file on Linux and UNIX systems.

Property and Values	Description
Basic options	
<code>install.etxcn.ListenPort=portnumber</code>	The port number for the Connection Node to use (default port: 5510).

Property and Values	Description
<code>install.etxcn.StartNow=1</code> or <code>0</code>	When set to 1, starts the Connection Node at the end of the installation (required for automatic node registration).
<code>install.etxcn.AllowMigrate=1</code> or <code>0</code> and <code>install.etxcn.MigrateFromThisFolder=full/path/to/old CN folder</code>	These two properties can be used to migrate from a previous version.
	When <code>install.etxcn.AllowMigrate</code> is set to 1, allows you to migrate the node from one version to the next. In this case, you must also set the <code>install.etxcn.MigrateFromThisFolder=full/path/to/old_folder</code> property.
	Note: Migrating from an existing node stops the node and terminates all running sessions on the node. If the node from which you are migrating is version 11.5 or later, migrating the node is no longer required. Node updates are pushed out by Exceed TurboX Server after you apply an update to the server.
<code>install.etxcn.SaveConnectionNodeIdToFile=1</code> or <code>0</code>	Legacy option for older Connection node versions.
<code>install.etxcn.CreateETXProxyUser=1</code> or <code>0</code>	When set to 1, creates the etxproxy user account if it does not exist.
<code>install.etxcn.CreateETXStartUser=1</code> or <code>0</code>	When set to 1, creates the etxstart user account if it does not exist.
Service flags	
<code>install.service.createservice=1</code> or <code>0</code>	When set to 1, create service <code>otetxcn service</code> . It is recommended NOT to turn this off.
<code>install.service.bBootStart=1</code> or <code>0</code>	When set to 1, enables running the node when the system starts.
Node registration flags	

Property and Values	Description
<code>install.register.bAutoRegister=1 or 0</code>	When set to 1, the system attempts to automatically register the Connection Node at the end of the installation.
<code>install.register.r_serverurl=https://yourserver.fqdn:port</code>	Specifies the URL to connect to for registration.
<code>install.register.r_overridehostname=fqdn.hostname</code>	Specifies the hostname for the Exceed TurboX site. This is the value displayed by the Server Manager as Host Name .
<code>install.register.r_proxy=1 or 0</code>	When set to 1, enables the Proxy Manager role.
<code>install.register.r_auth=1 or 0</code>	When set to 1, enables the Authentication role.
<code>install.register.r_appscan=1 or 0</code>	When set to 1, enables application scanning.
<code>install.register.r_firstdisplay= display=display</code>	The starting display number for the X server. Must be a positive integer (1 or greater).
<code>install.register.r_altnameserver= fqdn.hostname</code>	A fully qualified hostname to use to establish connections from the server to this host.
<code>install.register.r_altnameclient=fqdn.hostname</code>	A fully qualified hostname to use to establish connections from the clients to this host.
<code>install. register.r_additionaloptions</code>	Used for undocumented flags or recommended override values.
<code>install.register.r_resttoken= api_ key</code>	The API key to use for REST authentication when registering the node. This API key must have been created by a user with full administrator rights.
<code>install.register.r_maxtotalsessions=int</code>	The maximum number of active and suspended sessions that can run on this node at one time.
	The value must be either 0, indicating no limit, or a positive integer.

Property and Values	Description
<code>install.register.r_maxsessperuser= int</code>	The maximum number of active and suspended sessions that any one user can have on this node at one time.
	The value must be either 0, indicating no limit, or a positive integer.
<code>install.register.r_notes=string</code>	Enter a string that goes into the node information notes field. Do not include UNIX symbols such as " * & \$. If you want to include those symbols in a note, you can modify the note after installation using the Server Manager or the REST API.
<code>install.register.r_WebAdaptor= int</code>	Indicates whether to allow Web Client access on this node. Set to 1 to allow Web Client access or 0 not to.
<code>install.register.WebAdaptorPort= int</code>	When <code>install.register.r_WebAdaptor</code> is set to 1, set this to the port on which the Web Adaptor will listen for Web Client requests.
Installation flags	
<code>install.register.r_kerberoslib=/path/to/libkerb5</code>	This parameter overrides the default path to Kerberos libraries, as detected by the installer. In most cases, the default path will be correct and this parameter may be omitted. (Applicable to UNIX systems only.)
<code>install.register.r_gsslib=/path/to/libgssapi</code>	This parameter overrides the default path to Kerberos libraries, as detected by the installer. In most cases, the default path will be correct and this parameter may be omitted. (Applicable to UNIX systems only.)

For additional tasks you can perform, see the following topics:

- [Troubleshooting installation errors](#)
- [Registering a node](#)
- [Changing the node certificate](#)

Troubleshooting installation errors

If the installation was successful, the `bin/install` script returns `0` (success). If the script returns a number other than `0`, a failure has occurred. A failure may be the result of a bad response file or may be caused by other issues, such as user permissions.

If the installation fails, examine the installation logs to determine the case. Installation log files are saved to the `/installlogs` directory in the installer root folder.

Registering a node

When using PAM or Native authentication, you must install and register an authentication node before users can sign in to Exceed TurboX Server. The Exceed TurboX Server administrator can always sign in as the `etxadmin` user, to configure authentication and register or configure the authentication nodes.

When the node registration was successful, the node state is set to **Enabled** in the Server Manager.

To automatically register the node during an installation (silent or not), Exceed TurboX Server must be running and able to accept REST API requests and authenticate users. You cannot silently install the first native authentication Connection Node with automatic registration.

If you did not register the node automatically during the node installation, you can perform this step at a later time, provided that Exceed TurboX Server is running and able to accept REST API requests.

During the registration process you can do one of the following:

- Insert a token in the response file.
- Set the environment variable with the token.

Changing the node certificate

A self-signed SSL certificate is created during a silent installation. To use a custom certificate, either the installation must be migrated from a previous version or you can use the following steps.

To import an existing certificate:

1. Unpack the Connection Node into place.
2. Create customized `etxcert.pem` (public key) and `etxpriv.pem` (private key) files in `runtime/keys` (or links with `etxpriv.pem/etxcert.pem` naming).
3. Run the silent installation (it automatically skips the certificate generation and uses the customized `etxpriv.pem/etxcert.pem` files).

```
bin/install -s fullpath/responsefile
```