Using SSL Communication with Linux-Based Agent

You can secure communication between the Uptime monitoring station and the Uptime Linux agent by enabling SSL encryption. Enabling SSL is a two-step process:

- Enabling SSL on the Linux Agent System
- Enabling SSL in the Uptime UI

Enabling SSL on the Linux Agent System

To enable SSL encryption, complete the following steps on each agent system:

> **Note**
>
> Perform these steps on the Agents only. Do not perform these steps on the monitoring station.

1. Ensure Stunnel is installed on the agent server. If you do not have access to a distribution, you can download it from Stunnel.org.
2. Edit the /etc/xinetd.d/uptmagnt file so that it includes the following configuration information:

```
service uptmagnt
{
disable = no
flags = REUSE
socket_type = stream
wait = no
user = nobody
server = /usr/sbin/stunnel
server_args = /etc/stunnel/uptmagnt.conf
}
```

3. Create the certificate that will be used by Stunnel. For example:

```
openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
```

   The following is a sample stunnel.cnf for the openssl program:

```
# create RSA certs - Server
RANDFILE = stunnel.rnd
[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
[ req_dn ]
countryName = Country Name (2 letter code)
countryName_default = PL
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
0.organizationName_default = Stunnel Developers Ltd
organizationalUnitName = Organizational Unit Name (eg, section)
#organizationalUnitName_default =
0.commonName = Common Name (FQDN of your server)
0.commonName_default = localhost
# To create a certificate for more than one name uncomment:
# 1.commonName = DNS alias of your server
# 2.commonName = DNS alias of your server
# ...
# See http://home.netscape.com/eng/security/ssl_2.0_certificate.html
# to see how Netscape understands commonName.
[ cert_type ]
nsCertType = server
```

4. Copy stunnel.pem to /etc/stunnel/uptmagnt.pem.
   Create the /etc/stunnel/uptmagnt.conf file and add the following lines:

```
cert=/etc/stunnel/uptmagnt.pem
exec=/opt/uptime-agent/bin/uptmagnt
```

   Restart the xinetd service. After doing this, your agent should now be in SSL mode.

   You can verify that your agent is communicating securely by running the following command on your monitoring station:

```
agentcmd +s -p 9998 <hostname> df-k
```


Note

You can change the port on which to enable SSL to any value. To change the default agent port to something other than 9998, edit the /etc/services file, and restart xinetd. You can also use the agent-configure.sh script (see Changing Linux agent port or permissions for more information).

Enabling SSL in the Uptime UI

If the Linux agent has already been added to Uptime, complete the following steps in the Uptime Web interface for each agent system that you want to configure to use SSL.

1. Click **My Infrastructure**.
2. Click the name of the agent system for which you want to enable SSL.
3. On the system information page, click the **Edit Performance Monitor** link in the **System Profile** section.
4. In the new **Edit Service Monitor** window that appears, select the **Use SSL (HTTPS)** option.
5. Click **Save**.
   Once saved, your Monitoring Station and agent system will be communicating via SSL.

If you have not yet added the agent system to Uptime, follow the steps that are detailed in the *Uptime User Guide*. When adding the agent system, ensure that the **Agent Port Number** option is set to 9998, and that the **Use SSL (HTTPS)** option is enabled.