Installing Trust Agent as non-root user

# Configuration

There are required configuration settings that must be in the environment prior to running the installer.

MTWILSON\_API\_URL=https://10.1.68.33:8443/mtwilson/v2

MTWILSON\_API\_USERNAME=admin

MTWILSON\_API\_PASSWORD=password

MTWILSON\_TLS\_CERT\_SHA1=06d8cf367822b3ccf05c6311784ea8c126eb9b63

If you already have TPM ownership, you can also provide the TPM owner password in hex format so the trust agent can reuse it; without this, the TPM would need to be cleared for the trust agent to take ownership; without ownership the trust agent will not complete its setup procedure successfully.

REGISTER\_TPM\_PASSWORD=n

TPM\_OWNER\_SECRET=eaf68097599b5cbf66eac75e933ca7d738f2683d

The following variables must be defined in order to either install tagent as root and later run it as non-root

export TRUSTAGENT\_HOME=/opt/trustagent

export TRUSTAGENT\_USERNAME=tagent

# Actions to take as root before installation

## Disable monit temporarily

rm /etc/monit/conf.d/ta.monit

service monit restart

## Install required packages

### SUSE

Use either zypper or yast:

zypper install openssl libopenssl-devel libopenssl1\_0\_0 openssl-certs trousers-devel

yast -i openssl libopenssl-devel trousers trousers-devel tpm-tools make gcc unzip

### RedHat and Fedora

Use yum:

yum -y install openssl trousers trousers-devel tpm-tools make gcc unzip

Now check for missing libcrypto link, add if necessary:

has\_libcrypto=`find / -name libcrypto.so.1.0.0 | head -1`

libdir=`dirname $has\_libcrypto`

has\_libdir\_symlink=`find $libdir -name libcrypto.so`

has\_usrbin\_symlink=`find /usr/bin -name libcrypto.so`

if [ -n "$has\_libcrypto" ]; then

if [ -z "$has\_libdir\_symlink" ]; then

echo "Creating missing symlink for $has\_libcrypto"

ln -s $libdir/libcrypto.so.1.0.0 $libdir/libcrypto.so

fi

if [ -z "$has\_usrbin\_symlink" ]; then

echo "Creating missing symlink for $has\_libcrypto"

ln -s $libdir/libcrypto.so.1.0.0 /usr/lib/libcrypto.so

fi

ldconfig

fi

### Ubuntu

Use apt-get:

apt-get -y install openssl libssl-dev libtspi-dev libtspi1 trousers make gcc unzip

## Configure firewall

Ensure the system firewall has port 1443 open for trust agent

## Create Trust Agent User

mkdir -p $TRUSTAGENT\_HOME

chown -R $TRUSTAGENT\_USERNAME:$TRUSTAGENT\_USERNAME $TRUSTAGENT\_HOME

useradd --comment "Mt Wilson Trust Agent" --home $TRUSTAGENT\_HOME --system --shell /bin/bash $TRUSTAGENT\_USERNAME

## Configure authbind

The following commands allow trust agent to listen on port 1443:

mkdir -p /etc/authbind/byport

touch /etc/authbind/byport/1443

chown $TRUSTAGENT\_USERNAME /etc/authbind/byport/1443

chmod 500 /etc/authbind/byport/1443

## Update system information

Trust agent has a command for this (“tagent update-system-info”) which can be run as root, but this information is also needed during setup, so currently you must run the following commands as root before the first non-root install.

TRUSTAGENT\_VAR=$TRUSTAGENT\_HOME/var

mkdir -p $TRUSTAGENT\_VAR/system-info

dmidecode -s bios-vendor > $TRUSTAGENT\_VAR/system-info/dmidecode.bios-vendor

dmidecode -s bios-version > $TRUSTAGENT\_VAR/system-info/dmidecode.bios-version

dmidecode -s system-uuid > $TRUSTAGENT\_VAR/system-info/dmidecode.system-uuid

dmidecode --type processor > $TRUSTAGENT\_VAR/system-info/dmidecode.processor

lsb\_release -a > $TRUSTAGENT\_VAR/system-info/lsb\_release

virsh version > $TRUSTAGENT\_VAR/system-info/virsh.version

chown $TRUSTAGENT\_USERNAME:$TRUSTAGENT\_USERNAME $TRUSTAGENT\_VAR

# Run Trust Agent Installer as non-root

First copy the trustagent.env file into /opt/trustagent, then:

su - $TRUSTAGENT\_USER

export TRUSTAGENT\_HOME=/opt/trustagent

export TRUSTAGENT\_USERNAME=tagent

./mtwilson-trustagent-installer-2.0.6.bin

# Running Trust Agent as non-root

export PATH=$TRUSTAGENT\_HOME/bin:$PATH

tagent start

# Actions to take as root after installation

## Locking Trust Agent account

If you set up the trustagent to launch automatically as non-root on every reboot, or have a watchdog/supervisor process for ensuring that it’s running, so that you don’t need to login to the trustagent user account itself, then you should lock that account:

usermod --lock $TRUSTAGENT\_USERNAME -s /bin/false

## Register trust agent startup script (as root)

ln -s /opt/trustagent/bin/tagent /etc/init.d/tagent

### RedHat, Fedora, and SUSE

chkconfig --add tagent

### Ubuntu

updatercd tagent defaults

## Update system info automatically on every boot

crontab -l

Add the following line to the crontab, then save & exit:

@reboot tagent update-system-info

## Install and configure monit (as root)

TBD