Two factor authentication for OpenVPN SSL VPN

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine packaged to run within your corporate network. The LoginTC RADIUS Connector enables OpenVPN Community Software to use LoginTC for the most secure two-factor authentication.

Prerequisites

Before proceeding, please ensure you have the following:

RADIUS Domain Creation

If you have already created a LoginTC domain for your LoginTC RADIUS Connector, then you may skip this section and proceed to Installation.

1. Log in to LoginTC Admin
2. Click Domains:
3. Click Add Domain:
4. Enter domain information:

Name
Choose a name to identify your LoginTC domain to you and your users

Connector
RADIUS

Installation
The LoginTC RADIUS Connector runs CentOS 6.8 with SELinux. A firewall runs with the following open ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH access</td>
</tr>
<tr>
<td>1812</td>
<td>UDP</td>
<td>RADIUS authentication</td>
</tr>
<tr>
<td>1813</td>
<td>UDP</td>
<td>RADIUS accounting</td>
</tr>
<tr>
<td>8888</td>
<td>TCP</td>
<td>Web interface</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Web interface</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Web interface</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Package updates (outgoing)</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>NTP, Clock synchronization (outgoing)</td>
</tr>
</tbody>
</table>

Note: Username and Password

logintc-user is used for SSH and web access. The default password is logintcradius. You will be asked to change the default password on first boot of the appliance and will not be able to access the web interface unless it is change.

The logintc-user has sudo privileges.

Configuration

Configuration describes how the appliance will authenticate your RADIUS-speaking device with an optional first factor and LoginTC as a second factor. Each configuration has 4 Sections:

1. LoginTC

This section describes how the appliance itself authenticates against LoginTC Admin with your LoginTC organization and domain. Only users that are part of your organization and added to the domain configured will be able to authenticate.

2. First Factor

This section describes how the appliance will conduct an optional first factor. Either against an existing LDAP, Active Directory or RADIUS server. If no first factor is selected, then only LoginTC will be used for authentication (since there are 4-digit PIN and Passcode options that unlock the tokens to access your domains, LoginTC-only authentication this still provides two-factor authentication).

3. Passthrough
This section describes whether the appliance will perform a LoginTC challenge for an authenticating user. The default is to challenge all users. However with either a static list or Active Directory / LDAP Group you can control whom gets challenged to facilitate seamless testing and rollout.

4. Client and Encryption

This section describes which RADIUS-speaking device will be connecting to the appliance and whether to encrypt API Key, password and secret parameters.

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

The web interface makes setting up a configuration simple and straightforward. Each section has a Test feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

First Configuration

Close the console and navigate to your appliance web interface URL. Use username logintc-user and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

Create a new configuration file by clicking + Create your first configuration:

LoginTC Settings

Configure which LoginTC organization and domain to use:
Configuration values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>api_key</td>
<td>The 64-character organization API key</td>
</tr>
<tr>
<td>domain_id</td>
<td>The 40-character domain ID</td>
</tr>
</tbody>
</table>

The API key is found on the LoginTC Admin Settings page. The Domain ID is found on your domain settings page.

Click Test to validate the values and then click Next:

First Authentication Factor

Configure the first authentication factor to be used in conjunction with LoginTC. You may use Active Directory / LDAP or an existing RADIUS server. You may also opt not to use a first factor, in which case LoginTC will be the only authentication factor.
Active Directory / LDAP Option

Select **Active Directory** if you have an AD Server. For all other LDAP-speaking directory services, such as OpenDJ or OpenLDAP, select **LDAP**:

Configuration values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host or IP address of the LDAP server</td>
<td>ldap.example.com or 192.168.1.42</td>
</tr>
<tr>
<td>port (optional)</td>
<td>Port if LDAP server uses non-standard (i.e., 389 / 636 )</td>
<td>4000</td>
</tr>
<tr>
<td>bind_dn</td>
<td>DN of a user with read access to the directory</td>
<td>cn=admin,dc=example,dc=com</td>
</tr>
<tr>
<td>bind_password</td>
<td>The password for the above bind_dn account</td>
<td>password</td>
</tr>
<tr>
<td>base_dn</td>
<td>The top-level DN that you wish to query from</td>
<td>dc=example,dc=com</td>
</tr>
</tbody>
</table>
The attribute containing the user’s username
sAMAccountName or uid

The attribute containing the user’s real name
displayName or cn

The attribute containing the user’s email address
mail or email

Group Attribute (optional)
Specify an additional user group attribute to be returned the authenticating server.
4000

RADIUS Group Attribute (optional)
Name of RADIUS attribute to send back
Filter-Id

LDAP Group (optional)
The name of the LDAP group to be sent back to the authenticating server.
SSLVPN-Users

Encryption (optional)
Encryption mechanism
ssl or startTLS

CA certificate file (PEM format)
/opt/logintc/cacert.pem

Click Test to validate the values and then click Next.

Existing RADIUS Server Option
If you want to use your existing RADIUS server, select RADIUS:

Configuration values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host or IP address of the RADIUS server</td>
<td>radius.example.com or 192.168.1.43</td>
</tr>
<tr>
<td>port (optional)</td>
<td>Port if the RADIUS server uses non-standard (i.e., 1812)</td>
<td>1812</td>
</tr>
<tr>
<td>secret</td>
<td>The secret shared between the RADIUS server and the LoginTC RADIUS Connector</td>
<td>testing123</td>
</tr>
</tbody>
</table>
RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) found in the FreeRADIUS dictionary files will be relayed.

Click **Test** to validate the values and then click **Next**.

**Passthrough**

Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

For example, with smaller or proof of concept deployments select the **Static List** option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured **First Authentication Factor**. That means you will be able to test LoginTC without affecting existing users accessing your VPN.

For larger deployments you can elect to use the **Active Directory or LDAP Group** option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC your LDAP and Active Directory group policy will ensure that they will be challenged with LoginTC. Users not part of the group will only be challenged with the configured **First Authentication Factor**.

**No Passthrough (default)**

Select this option if you wish every user to be challenged with LoginTC.

**Static List**

Select this option if you wish to have a static list of users that will be challenged with LoginTC. Good for small number of users.
LoginTC challenge users: a new line separated list of usernames. For example:

```
jane.doe
jane.smith
john.doe
john.smith
```

**Active Directory / LDAP Group**

Select this option if you wish to have only users part of a particular Active Directory or LDAP group to be challenged with LoginTC. Good for medium and large number of users.

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginTC challenge auth groups</td>
<td>Comma separated list of groups for which users will be challenged with LoginTC</td>
<td>SSLVPN-Users or two-factor-users</td>
</tr>
<tr>
<td>Property</td>
<td>Explanation</td>
<td>Examples</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>host</td>
<td>Host or IP address of the LDAP server</td>
<td>ldap.example.com or 192.168.1.42</td>
</tr>
<tr>
<td>port (optional)</td>
<td>Port if LDAP server uses non-standard (i.e., 389 / 636)</td>
<td>4000</td>
</tr>
<tr>
<td>bind_dn</td>
<td>DN of a user with read access to the directory</td>
<td>cn=admin,dc=example,dc=com</td>
</tr>
<tr>
<td>bind_password</td>
<td>The password for the above bind_dn account</td>
<td>password</td>
</tr>
<tr>
<td>base_dn</td>
<td>The top-level DN that you wish to query from</td>
<td>dc=example,dc=com</td>
</tr>
<tr>
<td>attr_username</td>
<td>The attribute containing the user's username</td>
<td>sAMAccountName or uid</td>
</tr>
<tr>
<td>attr_name</td>
<td>The attribute containing the user's real name</td>
<td>displayName or cn</td>
</tr>
<tr>
<td>attr_email</td>
<td>The attribute containing the user's email address</td>
<td>mail or email</td>
</tr>
<tr>
<td>encryption</td>
<td>Encryption mechanism</td>
<td>ssl or startTLS</td>
</tr>
<tr>
<td>cacert (optional)</td>
<td>CA certificate file (PEM format)</td>
<td>/opt/logintc/cacert.pem</td>
</tr>
</tbody>
</table>

Configuration Simplified

If **Active Directory / LDAP Option** was selected in **First Authentication Factor** the non-sensitive values will be pre-populated to avoid retyping and potential typos.

Click **Test** to validate the values and then click **Next**.

Client and Encryption

Configure RADIUS client (e.g. your RADIUS-speaking VPN):
Client configuration values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A unique identifier of your RADIUS client</td>
<td>CorporateVPN</td>
</tr>
<tr>
<td>ip</td>
<td>The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)</td>
<td>192.168.1.44</td>
</tr>
<tr>
<td>secret</td>
<td>The secret shared between the LoginTC RADIUS Connector and its client</td>
<td>bigsecret</td>
</tr>
</tbody>
</table>

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

Click **Test** to validate the values and then click **Save**.
When you are ready to test your configuration, create a LoginTC user (if you haven’t already done so). The username should match your existing user. Provision a token by following the steps:

When you have loaded a token for your new user and domain, navigate to your appliance web interface URL:

Click Test Configuration:

Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:
Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

If there was an error during testing, the following will appear:

In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:
OpenVPN Configuration - Quick Guide

Once you are satisfied with your setup, configure your OpenVPN server to use the LoginTC RADIUS Connector.

For your reference, the appliance **web interface Settings** page displays the appliance IP address and RADIUS ports:

![LoginTC RADIUS Connector](image)

The instructions can be used for existing setups as well. For in depth instructions on setting up OpenVPN please see: OpenVPN Community Open Source Software Project.

**Centos**

1. Log In to your OpenVPN server.
2. Install **OpenVPN RADIUS plugin**:

   ```
   yum -y install libgcrypt libgcrypt-devel gcc-c++ make
   wget http://www.nongnu.org/radiusplugin/radiusplugin_v2.1a_beta1.tar.gz
   tar xvfz radiusplugin_v2.1a_beta1.tar.gz
   cd radiusplugin_v2.1a_beta1/
   make
   cp radiusplugin.so /etc/openvpn
   cp radiusplugin.cnf /etc/openvpn
   ```

3. Create OpenVPN server configuration file

   ```
   vi /etc/openvpn/server.conf
   ```
local 10.0.10.100
port 1194
proto udp
dev tun
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
cert /etc/openvpn/easy-rsa/2.0/keys/office.crt
key /etc/openvpn/easy-rsa/2.0/keys/office.key
dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem
plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radiusplugin.cnf
# plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so /etc/pam.d/login
client-cert-not-required
username-as-common-name
push "redirect-gateway def1"
server 10.0.10.0 255.255.255.0
push "dhcp-option WINS 10.0.10.1"
push "dhcp-option DNS 10.0.10.1"
ifconfig-pool-persist ipp.txt
client-to-client
duplicate-cn
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
log-append openvpn.log
verb 5
management localhost 7505
reneg-sec 0

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Address of OpenVPN server</td>
<td>10.0.10.100</td>
</tr>
<tr>
<td>ca</td>
<td>Location of root certificate</td>
<td>/etc/openvpn/easy-rsa/2.0/keys/ca.crt</td>
</tr>
<tr>
<td>cert</td>
<td>Location of OpenVPN server certificate</td>
<td>/etc/openvpn/easy-rsa/2.0/keys/office.crt</td>
</tr>
<tr>
<td>key</td>
<td>Location of OpenVPN server private key</td>
<td>/etc/openvpn/easy-rsa/2.0/keys/office.key</td>
</tr>
<tr>
<td>dh</td>
<td>Diffie hellman parameters</td>
<td>/etc/openvpn/easy-rsa/2.0/keys/dh1024.pem</td>
</tr>
<tr>
<td>server</td>
<td>VPN subnet for OpenVPN to draw client addresses from.</td>
<td>server 10.0.10.0 255.255.255.0</td>
</tr>
<tr>
<td>push</td>
<td>Push routes to the client to allow it to reach other private subnets behind the server.</td>
<td>&quot;dhcp-option WINS 10.0.10.1&quot;, &quot;dhcp-option DNS 10.0.10.1&quot;</td>
</tr>
</tbody>
</table>

For a more in-depth look at OpenVPN server configuration please consult: [Sample](#)
OpenVPN 2.0 configuration files.

4. Create RADIUS plugin configuration file

```bash
vi /etc/openvpn/radiusplugin.cnf:
```

```bash
NAS-Identifier=openvpn-server
Service-Type=5
Framed-Protocol=1
NAS-Port-Type=5
NAS-IP-Address=10.0.10.100
OpenVPNConfig=/etc/openvpn/server.conf
subnet=255.255.255.0
overwriteccfiles=true
nonfatalaccounting=false
server
{
    # The UDP port for radius accounting.
    acctport=1813
    # The UDP port for radius authentication.
    authport=1812
    # The name or ip address of the radius server.
    name=logintc-radius
    # How many times should the plugin send the if there is no response?
    retry=1
    # How long should the plugin wait for a response?
    wait=90
    # The shared secret.
    sharedsecret=bigsecret
}
```

<table>
<thead>
<tr>
<th>Property</th>
<th>Explanation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAS-Identifier</strong></td>
<td>The NAS identifier which is sent to the RADIUS server</td>
<td>openvpn-server</td>
</tr>
<tr>
<td><strong>Service-Type</strong></td>
<td>The service type which is sent to the RADIUS server</td>
<td>5</td>
</tr>
<tr>
<td><strong>Framed-Protocol</strong></td>
<td>The framed protocol which is sent to the RADIUS server</td>
<td>1</td>
</tr>
<tr>
<td><strong>NAS-Port-Type</strong></td>
<td>The NAS port type which is sent to the RADIUS server</td>
<td>5</td>
</tr>
<tr>
<td><strong>NAS-IP-Address</strong></td>
<td>The NAS IP address which is sent to the RADIUS server</td>
<td>10.0.10.100</td>
</tr>
<tr>
<td><strong>OpenVPNConfig</strong></td>
<td>Path to the OpenVPN config file</td>
<td>/etc/openvpn/server.conf</td>
</tr>
<tr>
<td><strong>subnet</strong></td>
<td>Support for topology option in OpenVPN 2.1</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td><strong>overwriteccfiles</strong></td>
<td>Allows the plugin to overwrite the client config in client config file directory</td>
<td>true</td>
</tr>
<tr>
<td>Property</td>
<td>Explanation</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>nonfatalaccounting</td>
<td>Allows the plugin to use auth control files if OpenVPN (&gt;= 2.1 rc8) provides them</td>
<td>false</td>
</tr>
<tr>
<td>server: acctport</td>
<td>The UDP port for radius accounting</td>
<td>1813</td>
</tr>
<tr>
<td>server: authport</td>
<td>The UDP port for radius authentication</td>
<td>1812</td>
</tr>
<tr>
<td>server: name</td>
<td>The name or ip address of the LoginTC RADIUS Connector</td>
<td>logintc-radius</td>
</tr>
<tr>
<td>server: retry</td>
<td>How many times should the plugin send the if there is no response?</td>
<td>1</td>
</tr>
<tr>
<td>server: wait</td>
<td>How long should the plugin wait for a response?</td>
<td>90</td>
</tr>
<tr>
<td>server: sharedsecret</td>
<td>The shared secret</td>
<td>bigsecret</td>
</tr>
</tbody>
</table>

For a more in-depth look at OpenVPN RADIUS plugin configuration please consult: GitHub: radiusplugin/radiusplugin.cnf.

5. Restart OpenVPN:

    service openvpn restart

To test, navigate to your OpenVPN clientless VPN portal or use OpenVPN Connect and attempt access.

**Troubleshooting**

**No Network Connection**

1. First ensure that your LoginTC RADIUS Connector is configured to have a virtual network adapter on eth0

2. Ensure that the virtual network adapter MAC address matches the one in the file /etc/sysconfig/network-scripts/ifcfg-eth0

3. Restart the networking service:

    service network restart

4. If you notice the error that eth0 is not enabled, then check driver messages for more information:

    dmesg | grep eth

5. It’s possible that the virtualization software renamed the network adapter to eth1. If this is the case, rename /etc/sysconfig/network-scripts/ifcfg-eth0 to ifcfg-eth1.

    mv /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth1
Open the file and update the `DEVICE="eth0"` line to `DEVICE="eth1"`

Not Authenticating

If you are unable to authenticate, navigate to your appliance web interface URL and click Status:

![LoginTC RADIUS Connector 2.1.0](image)

- All status checks have passed.
- Ping cloud.logintc.com
- RADIUS Process
- CPU Usage
- RAM Usage
- Disk Usage
- Version check

Ensure that all the status checks pass. For additional troubleshooting, click Logs:

![LoginTC RADIUS Connector 2.1.0](image)

- `/var/log/logintc/authenticate.log`
- `/var/log/radius/radius.log`
- `/var/log/logintc/tornado.log`

Displaying last 1000 lines, refreshes automatically every 1 second.

Email Support

For any additional help please email support@cyphercor.com. Expect a speedy reply.