Two factor authentication for RADIUS appliances

The LoginTC RADIUS Connector is a complete two-factor authentication virtual machine appliance packaged to run within your corporate network. The LoginTC RADIUS Connector allows your RADIUS-speaking corporate resources (e.g. VPNs) to use LoginTC for the most secure two-factor authentication. Supported devices include :

- Cisco ACS / ISE / ISR / Catalyst / IPSec VPN / SSH Network Device Access
- Citrix NetScaler Gateway (XenDesktop/XenApp)
- Palo Alto GlobalProtect / IPSEC VPN
- Juniper Networks Secure Access, Pulse Secure Connect Secure SSL VPN
- Dell SonicWALL NSA, TZ and Aventail (including Mobile Connect)
- VMware, Sohpos, F5, Pulse Secure, Array Networks, NetMotion

Any other appliances which have configurable RADIUS authentication are supported.

Since the LoginTC RADIUS Connector can speak RADIUS and LDAP it fits seamlessly into your existing setup without significant disruption. The appliance is configured to provide authentication to your existing RADIUS-speaking device and brokers first and second factor user authentication. The optional first factor is against an already existing LDAP, Active Directory or RADIUS device. The second factor is a secure authentication request to the user's mobile or desktop device.

The Appliance is very easy to configure with a rich web-based interface much like LoginTC Admin.

Authentication Flow

1. A user attempts access with their existing VPN client with username / password
2. A RADIUS authentication request is sent to the LoginTC RADIUS Connector
3. The username / password is verified against an existing first factor directory (LDAP, Active Directory or RADIUS)
4. An authentication request is made to LoginTC Cloud Services
5. Secure push notification request sent to the user's mobile or desktop device
6. User response (approval or denial of request) sent to LoginTC Cloud Services
7. The LoginTC RADIUS Connector polls until the user responds or a timeout is reached
8. RADIUS Access-Accept sent back to VPN
9. User is granted access to VPN

Architecture and Authentication Flow

Prerequisites

Before proceeding, please ensure you have the following:

RADIUS Domain Creation

Create a RADIUS domain in LoginTC Admin. The domain represents a service (e.g. VPN) that you want to protect with LoginTC. It will contain token policies and the users that access your service.

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 **Create Domain**:

   Create Domain

4. Enter domain information:

   Create Domain Form

Installation

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

Port	Protocol	Purpose
22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
443	TCP	Web interface
80	TCP	Web interface
80	TCP	Package updates (outgoing)
123	UDP	NTP, Clock synchronization (outgoing)

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:

Property	Explanation
api_key	The 64-character organization API key
domain_id	The 40-character domain ID

The API key is found on the LoginTC Admin <u>Settings</u> 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:

Property	Explanation	Examples
host	Host or IP address of the LDAP server	ldap.example.com or 192.168.1.42
port (optional)	Port if LDAP server uses non-standard (i.e., 389 / 636)	4000
bind_dn	DN of a user with read access to the directory	cn=admin,dc=example,dc=com
bind_password	The password for the above bind_dn account	password

Property	Explanation	Examples
base_dn	The top-level DN that you wish to query from	dc=example,dc=com
attr_username	The attribute containing the user's username	sAMAccountName or uid
attr_name	The attribute containing the user's real name	displayName or cn
attr_email	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
cacert (optional)	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**:

Web Server

Configuration values:

Property	Explanation	Examples
host	Host or IP address of the RADIUS server	radius.example.com or 192.168.1.43
port (optional)	Port if the RADIUS server uses non-standard (i.e., 1812)	1812
secret	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	testing123

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 <u>Static List</u> option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured <u>First Authentication Factor</u>. 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 <u>Active Directory or LDAP Group</u> 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 <u>First Authentication Factor</u>.

No Passthrough (default)

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

Web Server

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.

Web Server

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.

Web Server

Configuration values:

Property	Explanation	Examples
`LoginTC challenge auth groups`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users` or `two-factor-users`
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`

Property	Explanation	Examples
bind_dn	DN of a user with read access to the directory	cn=admin,dc=example,dc=com
bind_password	The password for the above bind_dn account	password
base_dn	The top-level DN that you wish to query from	dc=example,dc=com
attr_username	The attribute containing the user's username	sAMAccountName or uid
attr_name	The attribute containing the user's real name	displayName or cn
attr_email	The attribute containing the user's email address	mail or email
encryption (optional)	Encryption mechanism	ssl or startTLS
cacert (optional)	CA certificate file (PEM format)	/opt/logintc/cacert.pem

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):

Web Server

Client configuration values:

Property	Explanation	Examples
name	A unique identifier of your RADIUS client	CorporateVPN
ip	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	192.168.1.44
secret	The secret shared between the LoginTC RADIUS Connector and its client	bigsecret

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**.

Web Server

Testing

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:

Web Server

Click **Test Configuration**:

Web Server

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:

Web Server

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:

Web Server

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

Web Server

RADIUS Client Configuration

Once you are satisfied with your setup, configure your RADIUS device to use the LoginTC RADIUS Connector as its RADIUS authentication source. Set the RADIUS timeout to 90 seconds to allow enough time for LoginTC authentication responses.

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

Web Server

PAP Authentication

Your RADIUS client must use RADIUS PAP mode for authentication (which is usually the default). The LoginTC RADIUS Connector does not support CHAP, MS-CHAP, MS-CHAPv2, or EAP authentication modes.

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**:

Web Server

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

Web Server

Email Support

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