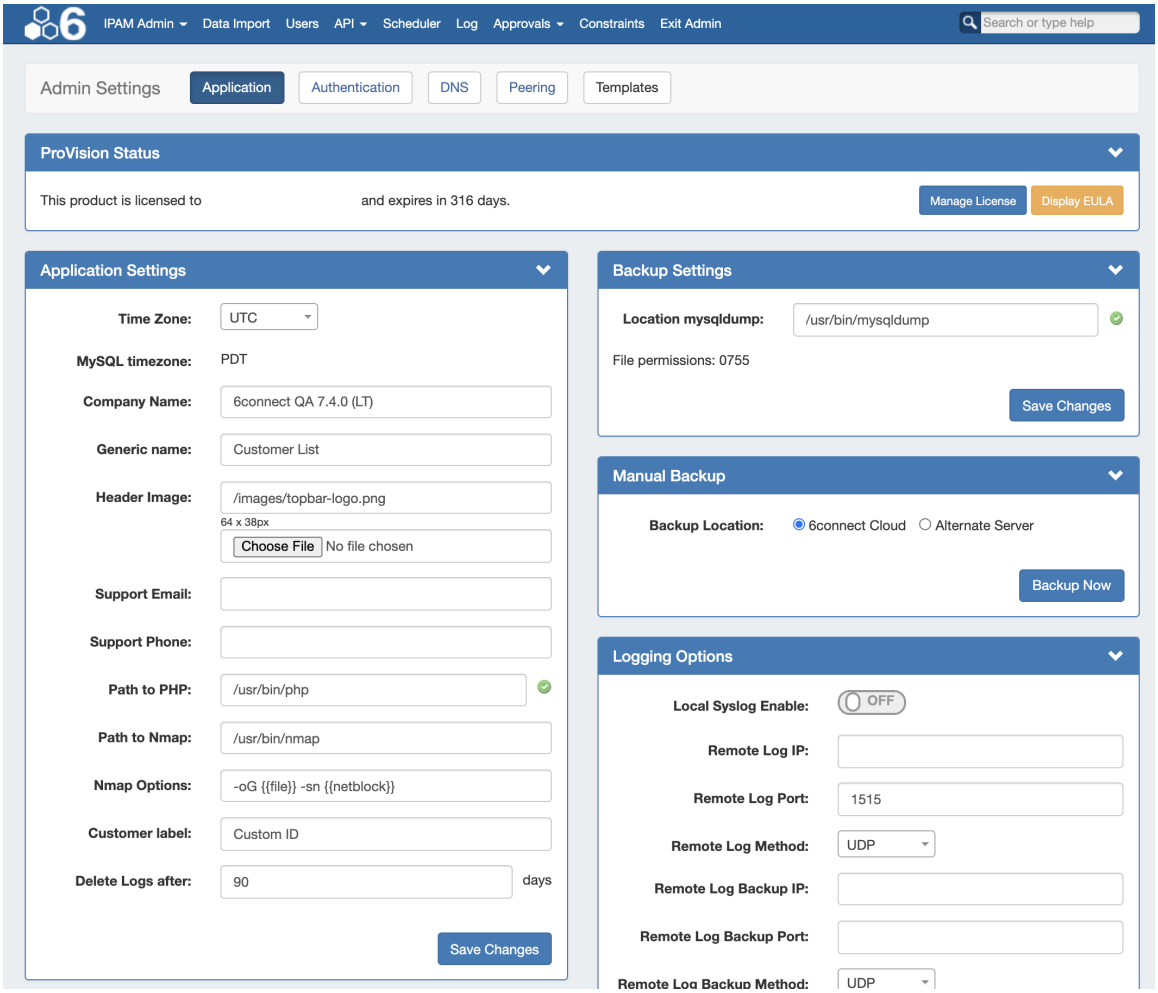
Admin Preferences

Overview



The Admin Preferences page is the home page of the Admin section of ProVision where general platform preferences may be set.

To access it, click the gear icon at the top right section of the header. From there, select "Admin". You will then have access the Admin section tabs of ProVision, and will see the Admin Preferences page. Each module area can be accessed by its own sub-tab button, available at the top of the page.

Video Walkthrough

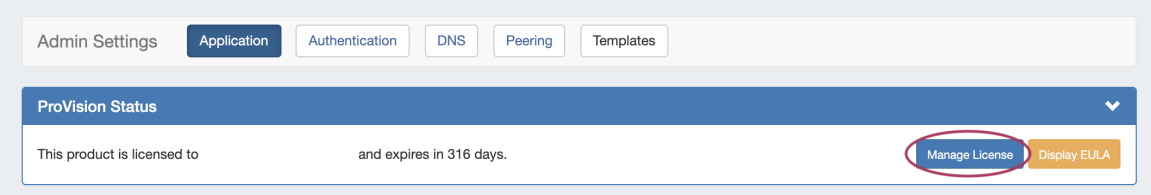
Note: Video at applies to versions 6.0.0 to 7.0.0. For earlier versions, see Admin Preferences Page Overview (v5.1.0+) .

Application Settings

License Info

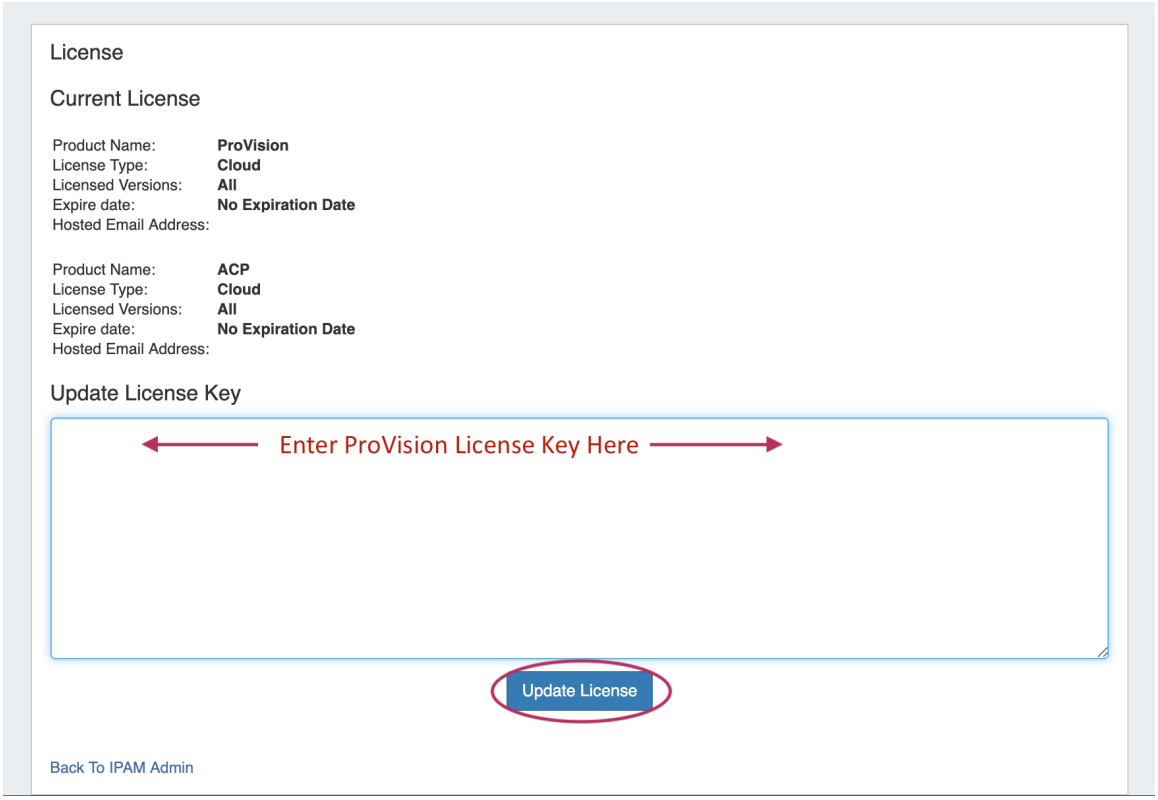
The License page displays current product license details such as Product, Type, Versions, Expiration, Email, and the option to add/update the 6connect License Key(s).

From the Admin Settings page, ensure the "Application" sub-tab is selected, then click "Manage License".



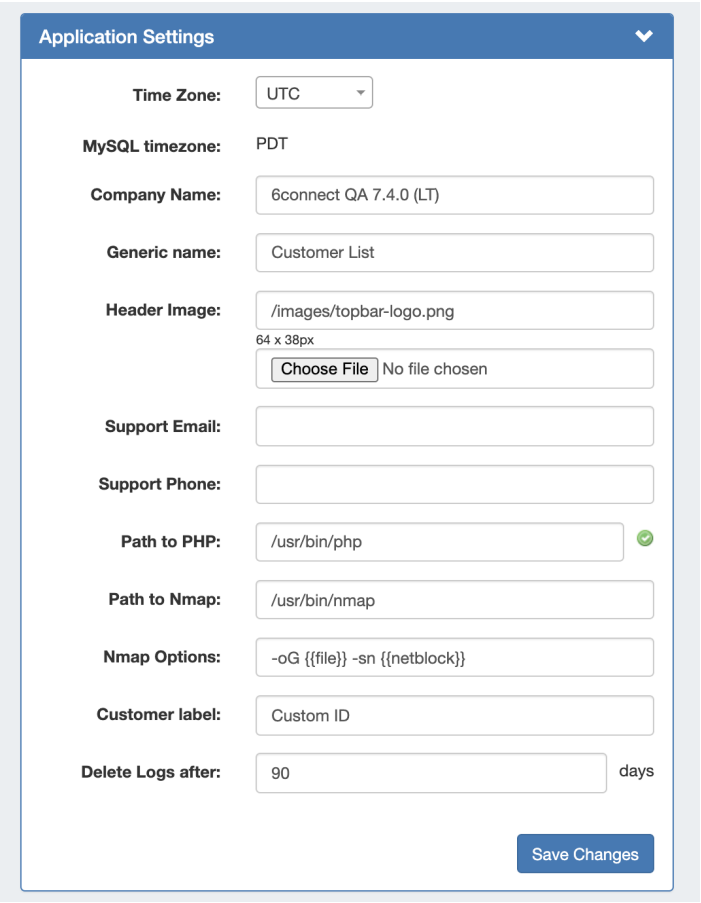
Current license details for ProVision, and other affiliated 6connect products will display.

To add/update a License Key, paste the key provided into the "Update License Key" box, and click "Update License".



Application Settings

Application Settings is where you provide company specific info that appears in the header and Dashboard.



Time Zone: Supported Time zones are listed here: {EXT} http://www.php.net/manual/en/timezones.php. Default value is ('America /Los_Angeles') and can be modified at any time via the drop down menu

MySQL Timezone: The timezone set from the server's MySQL settings.

Company Name: Enter the preferred name for your company to be used.

Generic Name: This "short" name is used in abbreviated location for the "Customer" tab label, "Customer" and "Site" are common entries.

Header Image: Select an image file for the header

Support Email: Support Email address that displays on the Dashboard

Support Phone: Support phone number that displays on the Dashboard

Path to PHP (Local Installation): The directory path to php location

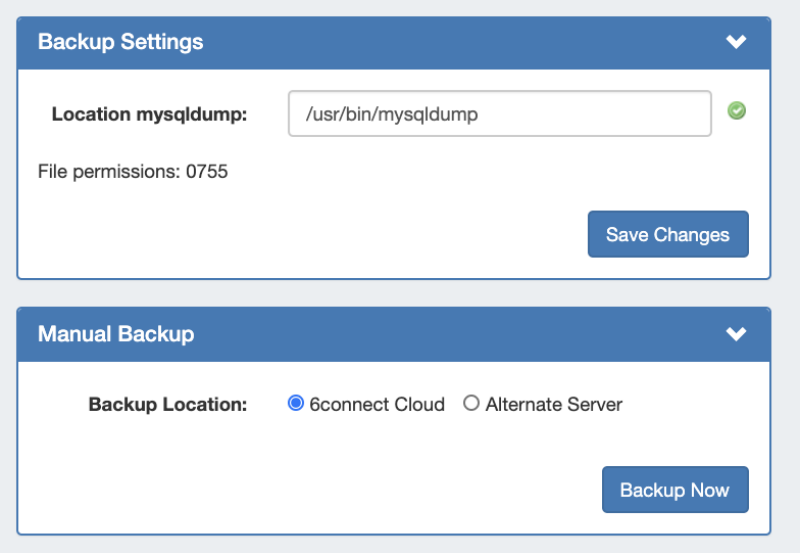
Path to Nmap (Local Installation): The directory path to nmap location

Nmap Options (Local Installation): Custom nmap options

Customer Label: The display name for the customizable label field available when creating or editing a resource.

Delete Logs after: The number of days to retain logs.

Backup Settings



For cloud users, regular backups can be set up through the Scheduler. However, prior to imports or other large changes, you may wish to manually perform a backup.

Backup Location: The backups may be sent to the 6connect cloud, or to a specific server in the Resource system. Select the radio button for the desired location.

Manual Backup - 6connect Cloud:

Select "6connect Cloud" as your backup location, then click on the "Backup Now" button. You will see a success message below the button if successful.

Manual Backup - Alternate Server:

Manual Backup: Alternate Server saves a backup msql dump to a Server Resource already set up in ProVision.

This Resource needs to have the following information provided in the server section fields in order to establish a connection: Port, Hostname, Username, and Password.

Before selecting Alternate Server Backup:

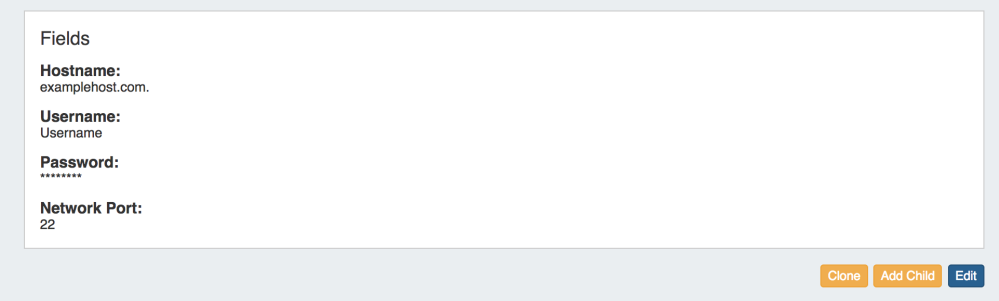
1) Ensure that the Server Resource exists in ProVision for the backup (Section = "Server"). If needed, create a new entry for the server.

2) Check that the following fields are added to the Server Section:

- Network Port (22 is typical)
- Hostname (this can also be an IP address)
- Username
- Password

See Customizing Sections and Customizing Fields for information on adding fields to sections. Hostname, Username, Password, and Network Port will all be contained under the "Existing Fields" selector when adding fields to the Section.

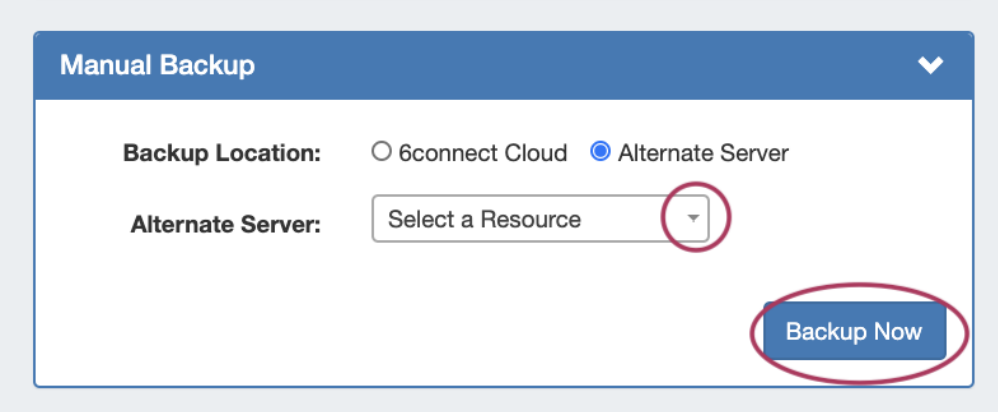
3) On the Backup Server's Entry page, verify that the server fields are filled in and correct for the ProVision server entry:



If needed, click "Edit" and add or update the information. See Working with Entries for additional information.

Once a Backup server has been set up in ProVision, it will be available to select under Backup Settings: Alternate Server.

Select "Alternate Server" as your backup location, then select the desired ProVision server Resource. After selecting your server, click on the "Backup Now" Button.

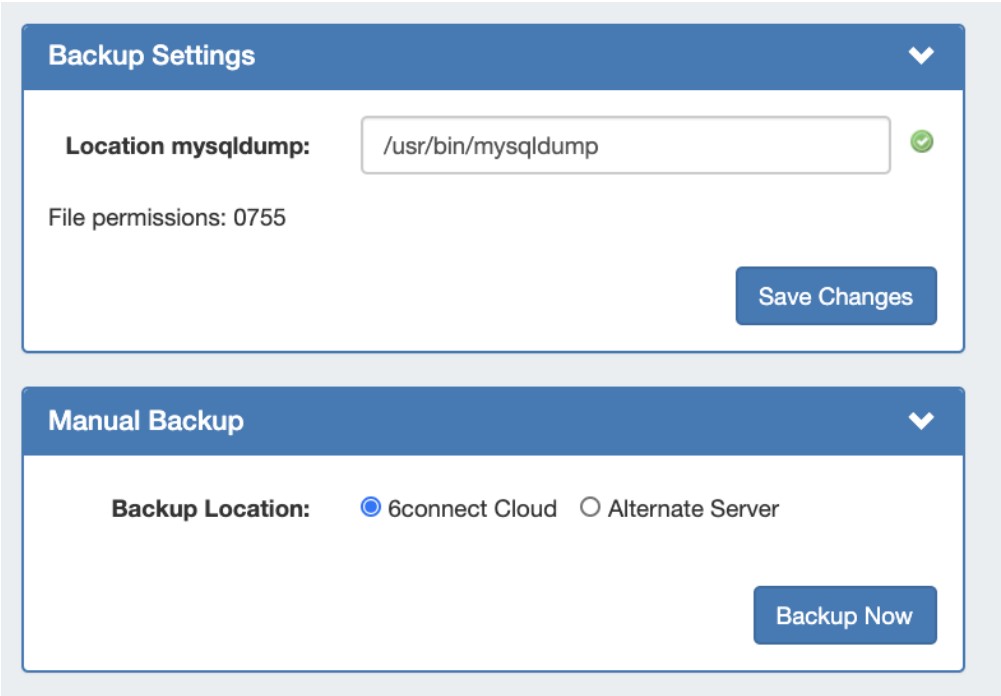


If successful, a mysql dump file will be sent to the selected server and a "Success!" message will appear.

Once the connection is confirmed successful, Backups to alternate servers may be scheduled on a recurring basis through the Scheduler Tab, or continued to be performed manually under Backup Settings.

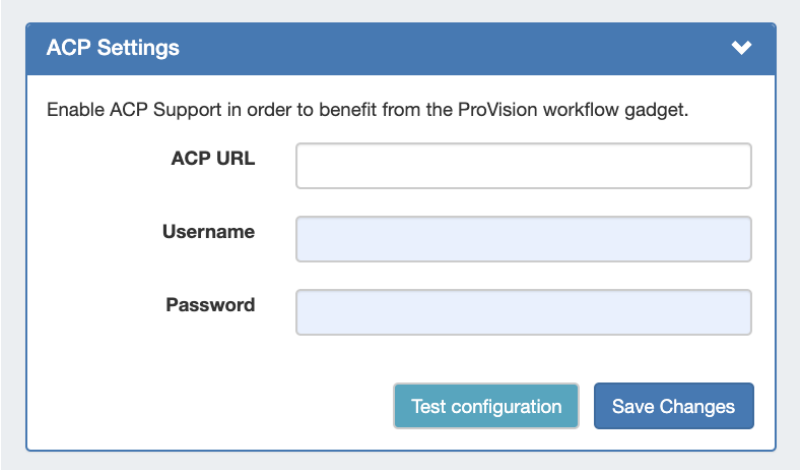
Backup Settings - Local Installation

Additional settings are available for local installations:



Location of mysqldump (Local Installation): This is the location of the mysqldump directory.

ACP Settings

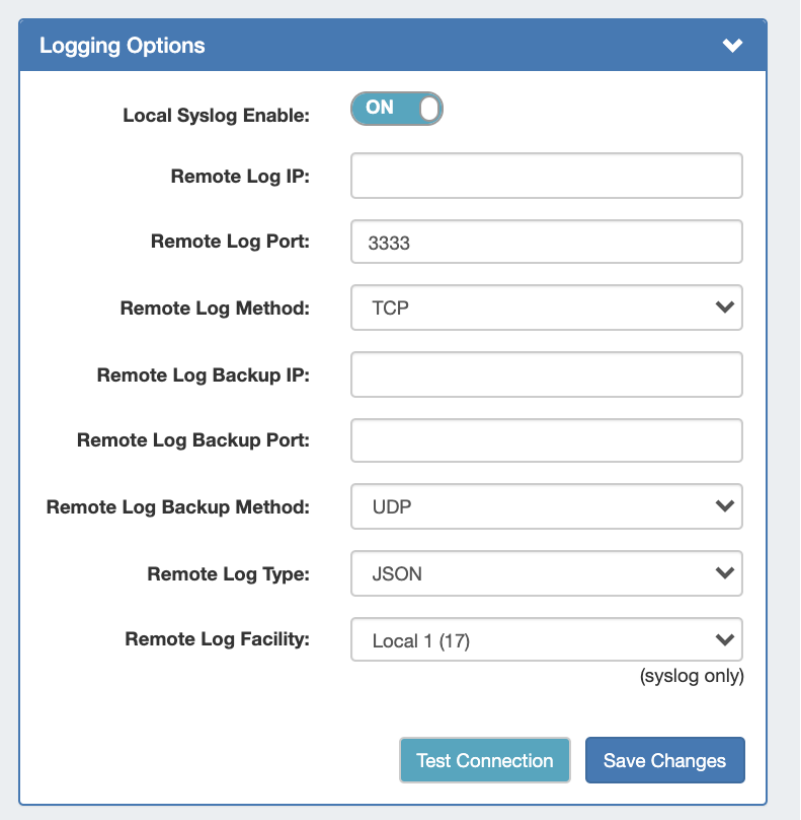


The ACP Settings area links an ACP instance and login credentials to the ProVision instance, and allows the ACP Workflow Gadget to execute Workflows as the provided user.

Enter the ACP URL for a licensed ACP instance, then provide the ACP Username and Password for the user that should be used to execute Workflows. To verify the account, click "Test Configuration" - you will be notified whether the account is valid.

When done, click "Test configuration" to verify the connection and then "Save Changes". Afterwards, you may proceed to configure the ACP Workflows Gadget to specify Workflows to execute in ProVision.

Logging Options



Remote Log IP: Target IP address that we will send log information to

Remote Log Port: Port number for the syslog server you will send log information to

Remote Log Method: Select TCP, UDP, SSL from the dropdown for the log delivery method

Remote Log Backup IP: Target IP address for the Backup syslog server you will send log information to

Remote Log Backup Port: Port number for the Backup syslog server you will send log information to

Remote Log Backup Method: Select TCP, UDP, SSL from the dropdown for the log delivery method

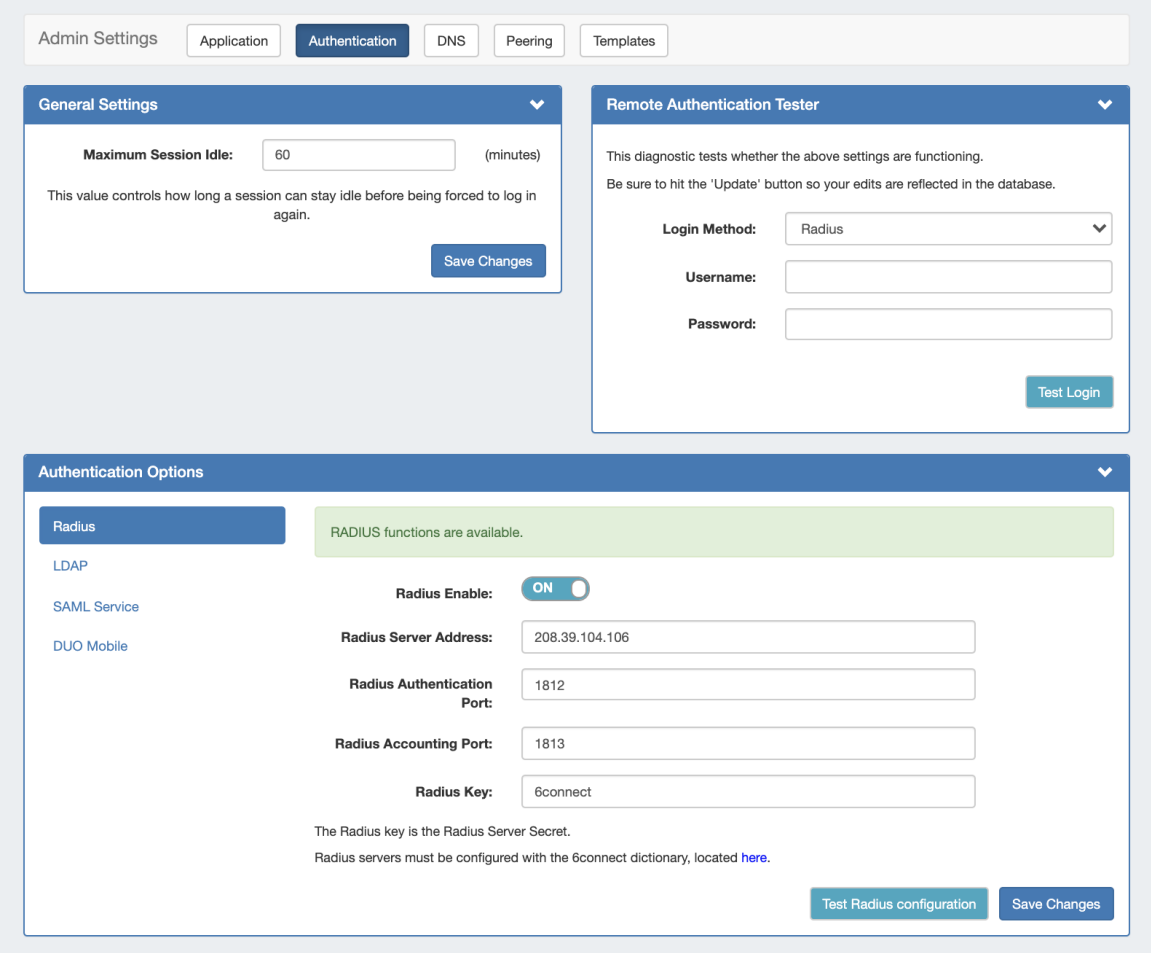
Remote Log Type: Select SysLog format or JSON output

Remote Log Facility: Select the Facility - applies to syslog only

If desired, you may select "Test Connection" to verify the connection before clicking "Save Changes".

Authentication Settings

Authentication options are accessed by clicking the "Authentication" sub-tab at the top of the Admin Preferences page.



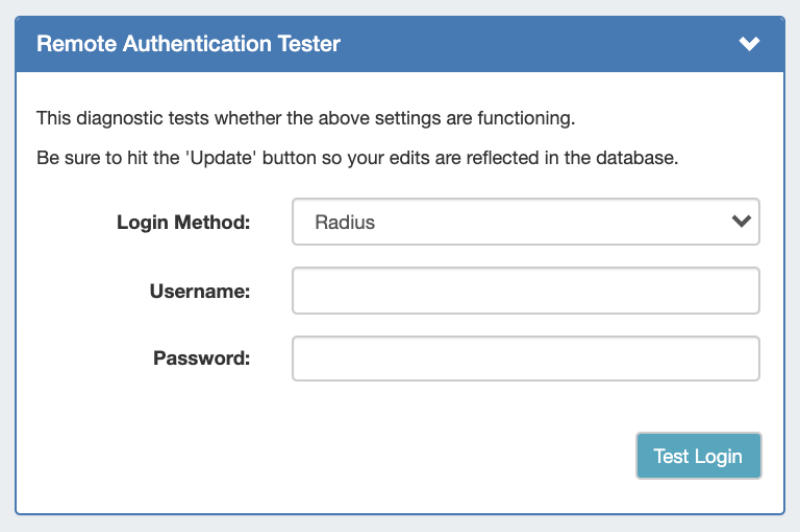
In this area, you may set the max session idle time, as well as setup additional authentication options.

Four authentication types are available for ProVision: Radius, LDAP, SAML, and DUO Mobile.

General Settings

Maximum Session Idle: This setting (minutes) controls how long a session can stay idle before being forced to log in again.

Remote Authentication Tester



The Remote Authentication Tester checks Radius / LDAP settings for a user.

Select the Login Method (Radius or LDAP), enter the Username and Password for the user, and then click "Test Login".

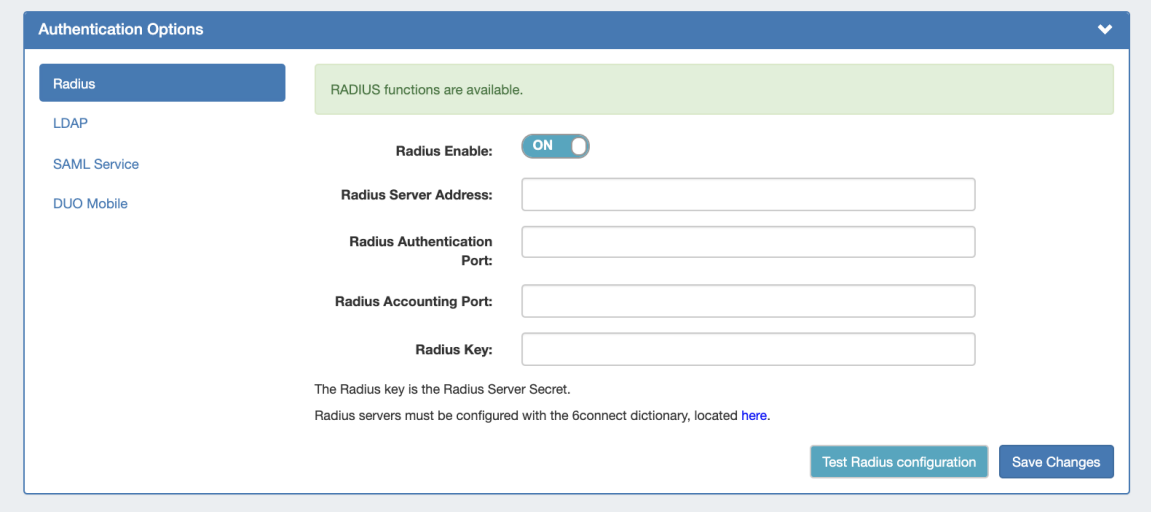
Login Method: Select Radius or LDAP, according to your authentication settings.

Username: The username for the user you are testing.

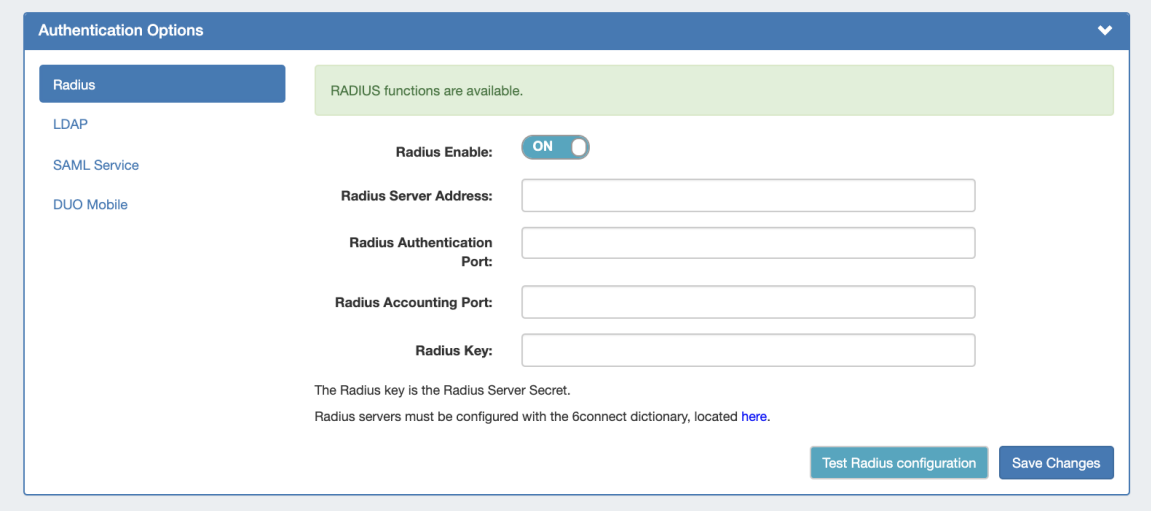
Password: Password for the user you are testing.

Authentication Options

Four authentication types are available for ProVision: Radius, LDAP, SAML, and DUO Mobile. To view settings for each, select the authentication type from the list at the left of the module.



RADIUS authentication options (local install only)



Note: For implementation details, go here.

Radius Enable: Check this box to enable RADIUS functionality.

Radius Server Address: Set to the IP address of your radius server. If this is specified, it will force authentication over radius.

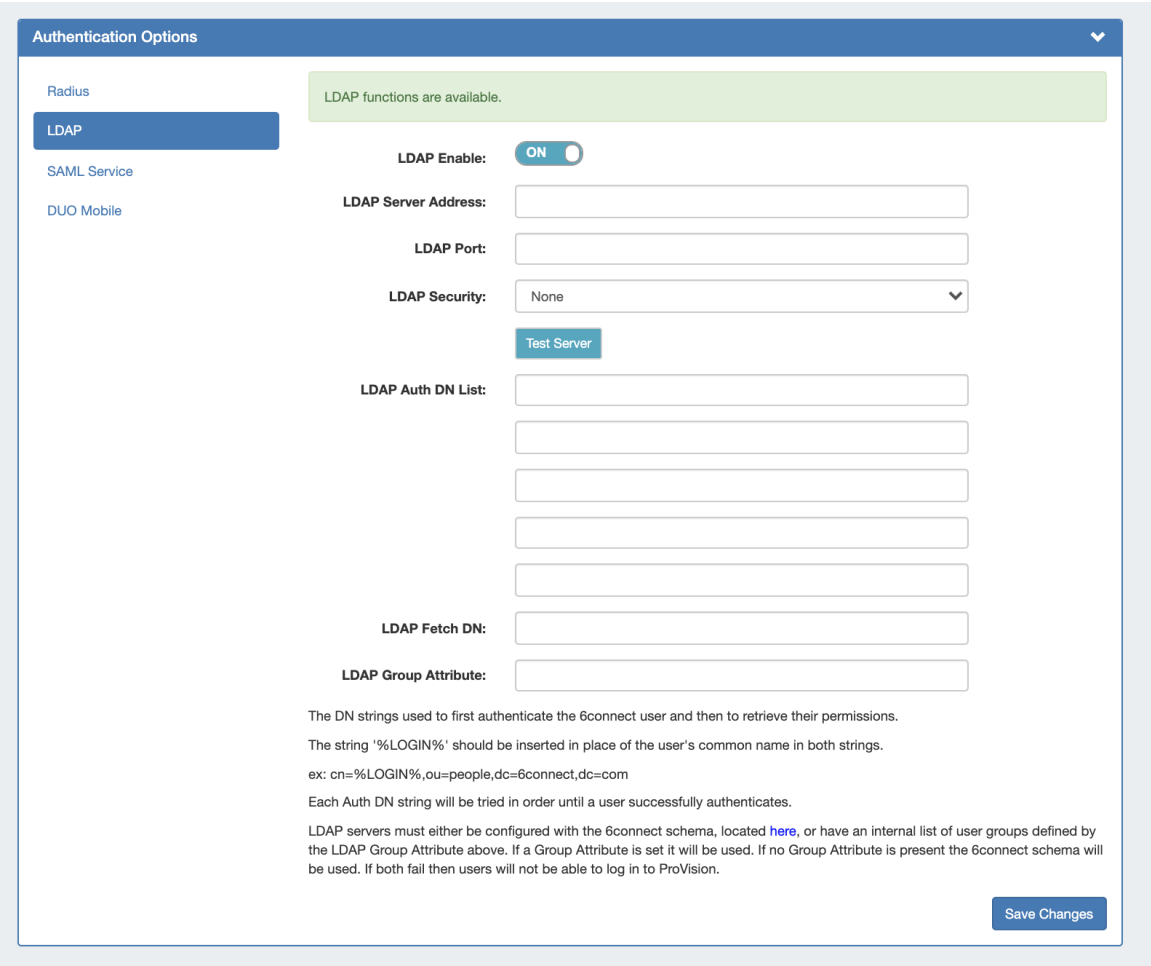
Radius Authentication Port: Set to the port for authentication. Default port is 1812

Radius Accounting Port: Set to the port for radius accounting. Default port is 1813

Radius Key: Set to the shared key of your radius server

To verify the settings connect, click "Test Radius Configuration". When done, click "Save Changes".

LDAP authentication



Note: For implementation details, go here.

LDAP Enable: check the box to enable LDAP functionality.

LDAP Server Address: Set the IP address of your LDAP server.

LDAP Port: Set the port for your LDAP server

LDAP Security: Select the security method of your LDAP server - SSL, TLS or None

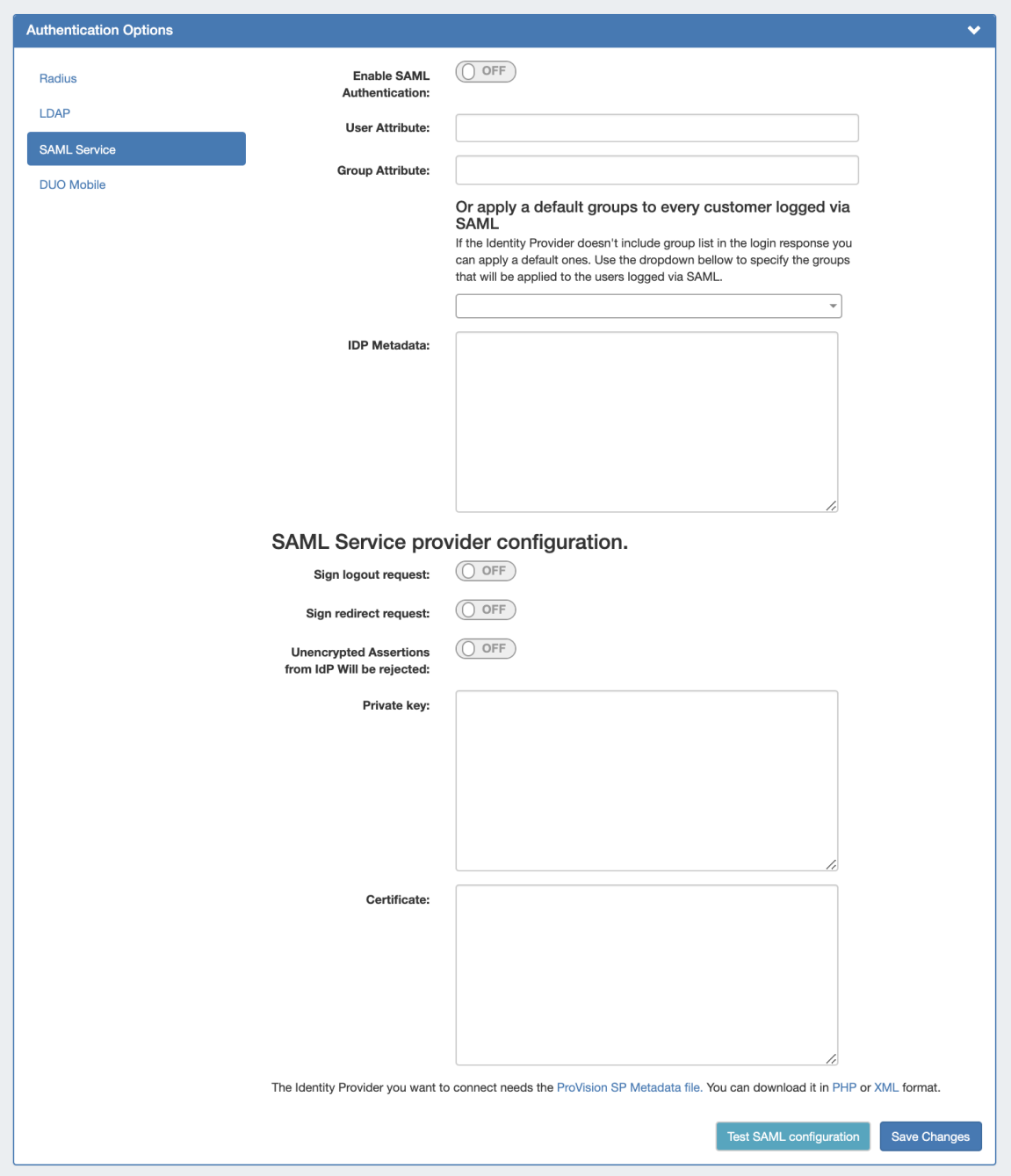
Test Server: Click to test the connection to the LDAP server.

LDAP Auth DN/Fetch DN: These strings are used to first authentication the 6connect user and then to retrieve their permissions. The string '% LOGIN%' should be inserted in place of the user's common name both strings. (ex: cn=%LOGIN%,ou=people,dc=6connect,dc=com)

LDAP Group Attribute: If using an internal list of user groups instead of 6connect groups, enter the attribute name for the LDAP groups here. If a Group Attribute is set, it will be used first, otherwise the 6connect schema will be used.

Mapping Permissions to 6connect schema: To integrate 6connect permissions with your existing directory structure then you will need the 6connect schema. It should snap in with any existing LDAP structure and allow you to assign 6connect permissions to your existing users. You can download a copy of the schema from this section.

SAML authentication



SAML is a Single Sign On (SSO) authentication method that uses an external identity provider to authenticate a user at their first login, saving a token to the user's browser that is then used for subsequent logins, so that the user does not need to re-submit credentials.

SAML Setup

Before configuring SAML in ProVision, you must have an account set up with an Identity Provider (IdP) and ProVision users / groups set up in the IdP.

Set up the IdP

To use SAML authentication, you will need SAML set up for your instance with an Identity Provider (IdP), such as *Microsoft ADFS, OneLogin, Elastic SSO,* or others. You can view a list of available SAML IdPs at Wikipedia's SAML based products page.

Users and Permissions:

User credentials will need to be created and associated with ProVision permission group names via the IdP. All user creation, management and permissions handling occurs via the IdP, externally from ProVision.

Configure SAML in ProVision

ProVision setup for SAML is located in **Admin** **Admin Settings** Authentication Options.

Under **SAML Configuration**:

Enable SAML authentication by clicking the checkbox next to "Enable".

The following fields are required and will need to be obtained from the IdP:

- **User Attribute(Required):**
- **Group Attribute(Required):**
- **IdP Metadata(Required):**

Under **SAML Service Provider Configuration:**

- **Sign logout request:**
- **Sign redirect request:**
- **Unencrypted Assertions from IdP Will be rejected:**
- **Private Key:**
- **Certificate (Required):**

Links are provided below the configuration settings for the ProVision SP Metadata file in php and xml format, which will be needed to provide to the IdP.

You can test the configuration by clicking the "Test SAML Configuration" button, a new page will open giving health check information for your provided attributes.

SAML Login

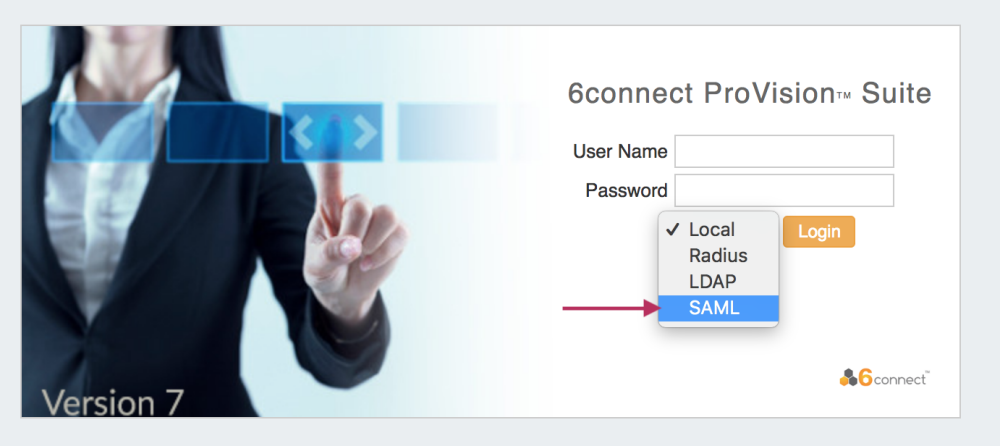
Once the correct configuration has been established and users set up for SAML in the IdP, users will be able to use SAML logins.

> Documentation Note: Depending on the IdP used, some screens may appear different from what is shown here.

Initial Login:

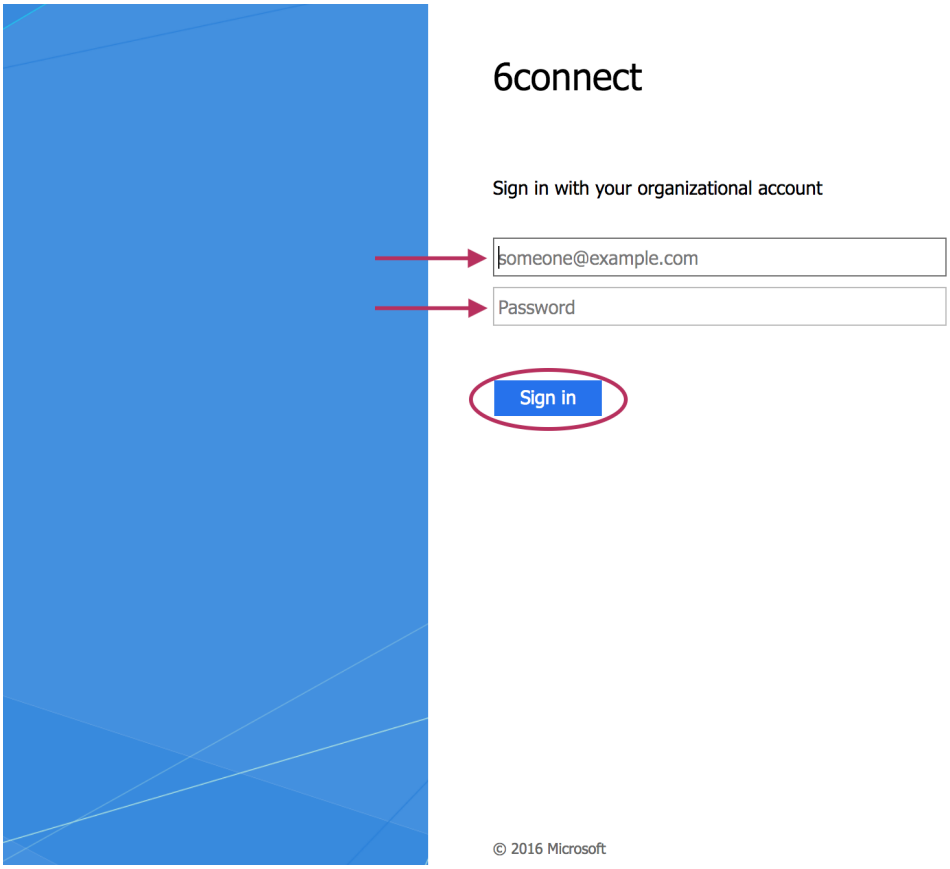
The initial login process occurs for the first time a user logs in, and anytime afterwards if the browser token is not present (e.g., cookies are cleared from the browser, the browser closed, or a new browser is used).

From the ProVision login page, select SAML from the authentication options dropdown - you do not need to enter Username or Password.



You will be redirected to the IdP site as set up in the Admin Configuration - here, we are using Microsoft ADFS (Active Directory Federation Services).

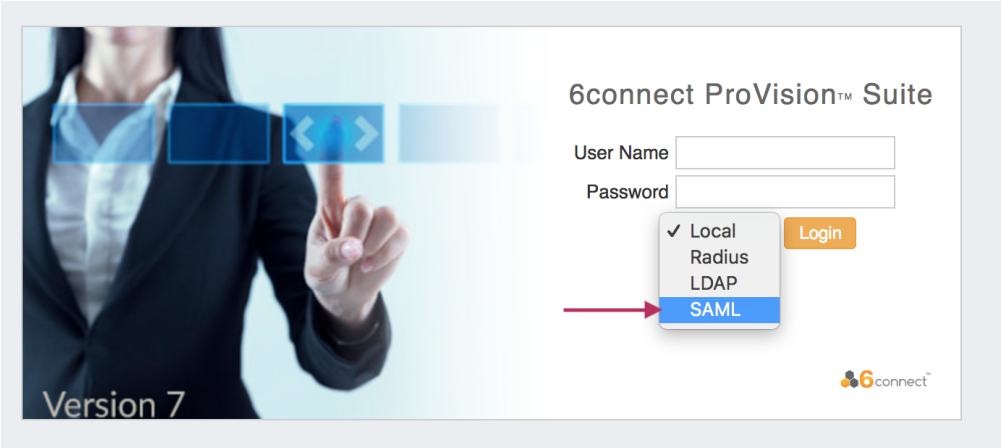
Log into the IdP site using your SAML credentials, and click "Sign In".



If the sign in is successful, you will be logged into the ProVision home page.

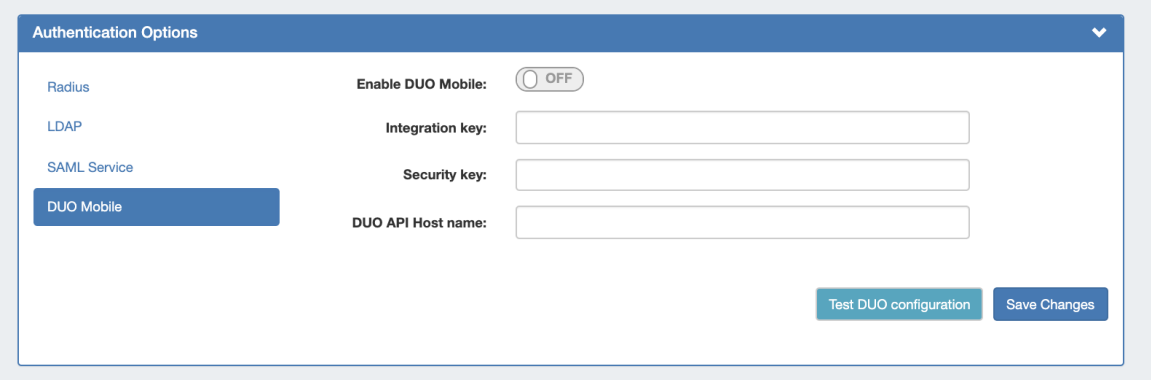
Subsequent Logins:

After the initial login via the IdP (as long as the auth token is present) users will be able to login to ProVision simply by selecting the "SAML" options from the ProVision login page without entering credentials.



The auth token may be destroyed or not available if browser cookies have been cleared, a different browser used, or the browser fully closed, depending on security settings. In these cases, the user will need to sign in again via the IdP.

DUO Mobile



To use DUO Authentication, an account must first be set up with DUO.

Once an account is set up, obtain the Integration Key, Security Key, and DUO API Host name.

Enter those items into **Admin** **Authentication Options** DUO Mobile Configuration, and click "Update" to save your changes.

You may also test the current configuration by clicking "Test DUO Configuration".

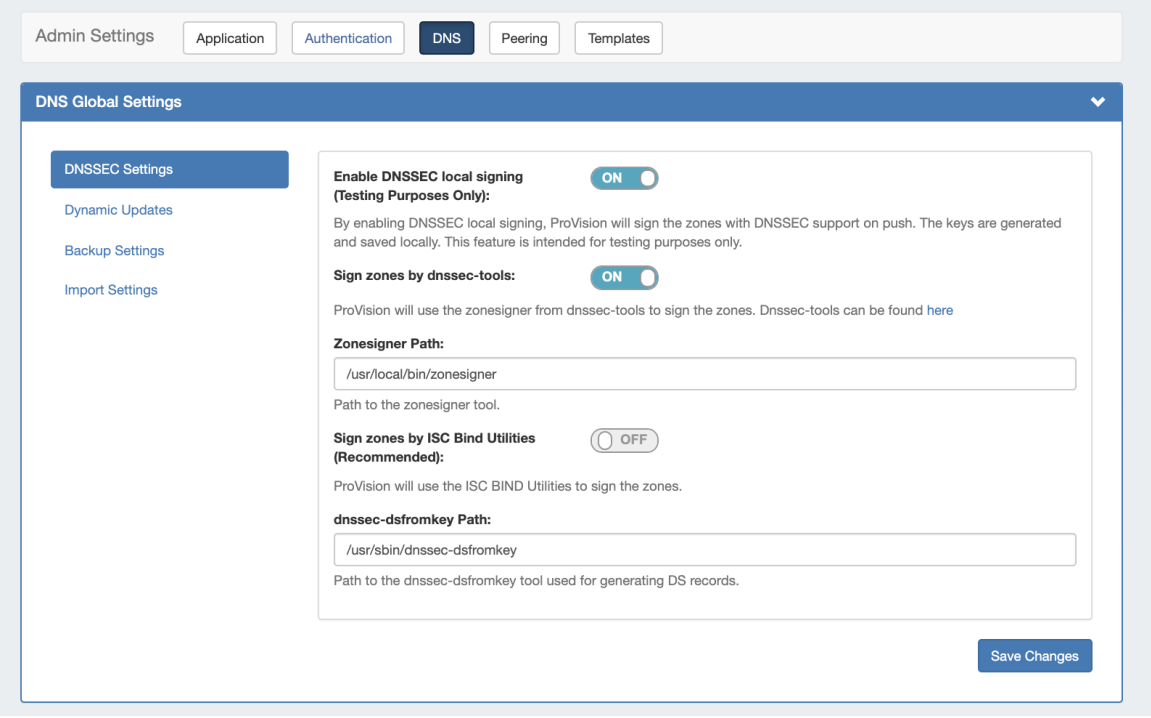
If you need to disable DUO Mobile authentication from ProVision from outside of the GUI, a command-line disable tool is available. Run:

```
php tools/disable_duo.php
```

DNS Settings

DNS Settings are accessed by clicking the "DNS" sub-tab at the top of the Admin Preferences page.

DNSSEC Settings



If using DNSSEC, select whether to enabled DNSSEC local signing, or sign zones by dnssec-tools, then enter the following information:

zonesigner path : Enter the zonesigner path that will be used for DNS. Zonesigner is required if dnssec-keygen and dnssec-signzone are not set.

Sign zones by ISC BIND Utilities: Select whether to use ISC BIND utilities to sign zones.

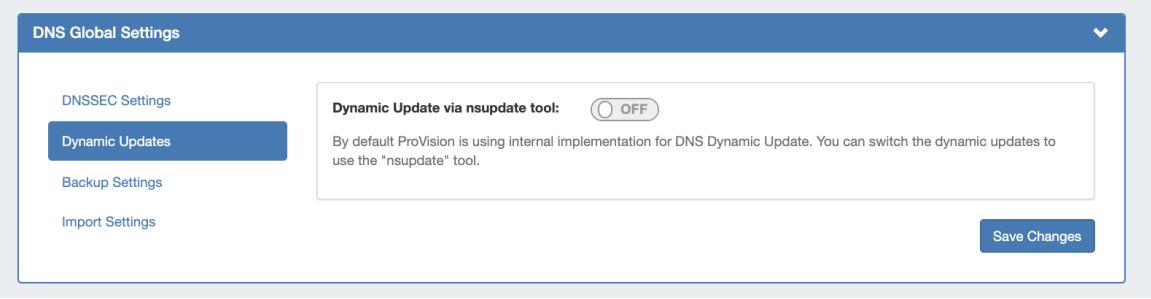
dnssec-dsfromkey path : Enter the dnssec-dsfromkey path that will be used for DNS. Required in all cases.

Additional Entropy

If delays occur due to lack of available entropy on servers, see the following article on how to set up additional entropy using haveged here:

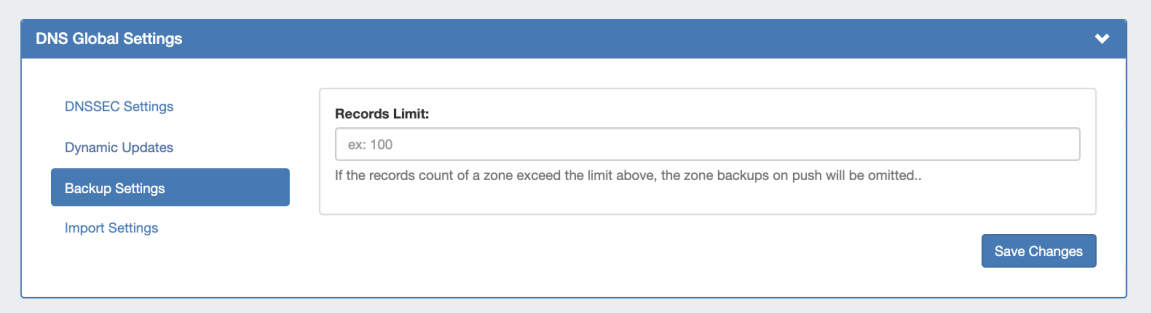
https://www.digitalocean.com/community/tutorials/how-to-setup-additional-entropy-for-cloud-servers-using-haveged

DNS Dynamic Update Settings



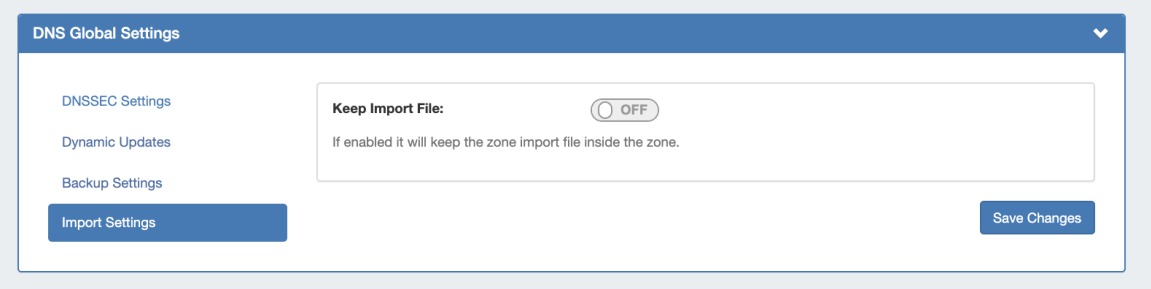
Dynamic Update via nsupdate: Toggle to "On" if you wish to use Dynamic Updates via nsupdate, instead of ProVision's internal implementation.

DNS Backup Settings



Records Limit : The limit for the number of records a zone may have for a zone to process a backup. If the records count exceed this number, zone backups will be omitted at zone push.

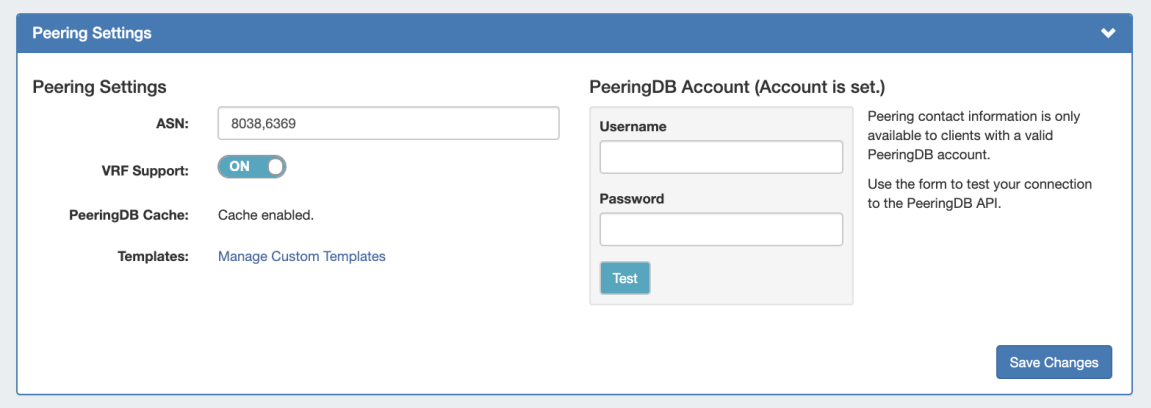
DNS Import Settings



Keep Import File: Toggle to "on" if you wish to retain the zone import file inside the zone.

Peering Settings

Peering Settings are accessed by clicking the "Peering" sub-tab at the top of the Admin Preferences page.



ASN : Enter the ASN(s) that will be used for Peering, or may leave blank. Separate multiple ASNs with a comma.

VRF Support: Check to enable adding the VRF gadget to the router Section. Currently, only supports Cisco routers.

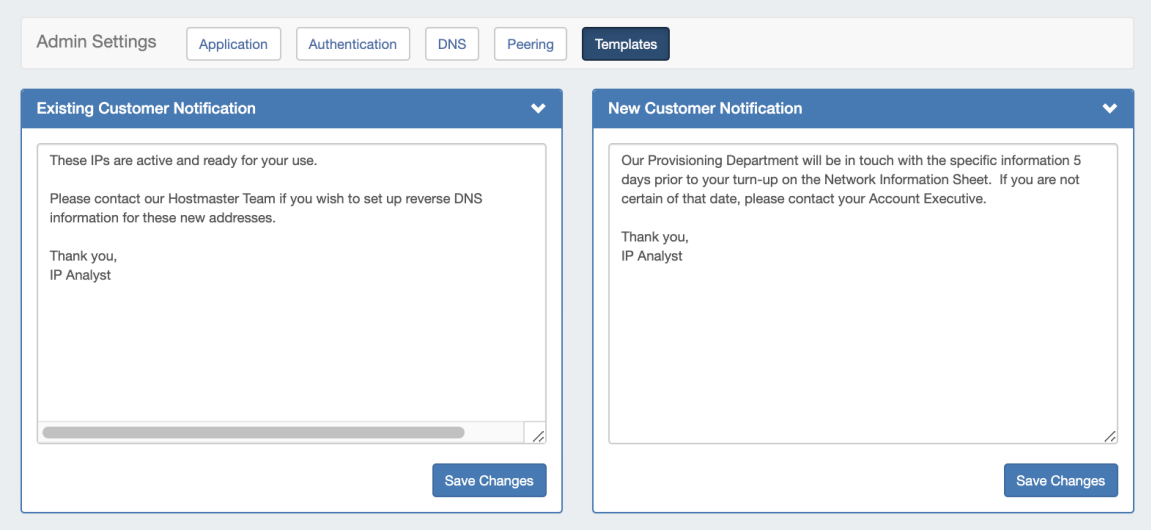
PeeringDB Cache: Displays a status notification to show whether Peering DB cache is enabled or disabled.

Templates: Create or manage custom Peering Templates.

PeeringDB Account: Click the "change" link to input PeeringDB account credentials. PeeringDB account information is required to retrieve and update peering information. Enter a valid PeeringDB account Username and Password. When done, click the "Test" button to verify the account, and save.

Templates

Email Templates are accessed by clicking the "Templates" sub-tab at the top of the Admin Preferences page.



This is where you can edit outgoing email templates for IP block assignments.

To edit, click inside the text area box, make the desired changes, then click the "Save Changes" button.