

Azara



Managed Services Provider

User's Guide

TABLE OF CONTENTS

Chapter 1, MSP Management

- 1.1 Tenant Management 1-2
- 1.2 MSP Logs 1-6
- 1.3 MSP Operations 1-8
 - 1.3.1 MSP Users 1-9
 - 1.3.2 MSP Preferences 1-14
 - 1.3.3 Two Factor Authentication 1-16

Appendix A, Customer Support

CHAPTER 1

MSP MANAGEMENT

Managed Services Providers (MSPs) are Extreme Networks partners and re-sellers who re-brand (white label) Azara Cloud service for their end users. MSP's end users are small to medium sized businesses and Enterprises that lack the know-how and personnel to deploy and manage *Wireless Local Area Networks* (WLANs) internally. MSPs bridge this gap by providing a Extreme Networks-powered, branded cloud offering along with day-to-day network management assistance. MSP's end users are referred to as Tenants. The Tenants in turn deploy Azara-managed networks consisting of one or more sites. Each site within the Tenant's network has access point deployed to provide clients with access to services provided by Azara.

MSPs perform various tasks including managing Tenants and administer MSP user accounts. The following tasks can be performed:

- **Manage Tenants:** View, add, modify, remove Tenant accounts. By default, the MSP account opens at the Tenants screen.
- **View Logs:** View and monitor the Azara service usage and operations at the MSP account level. Navigate to the Logs screen to review customer activities, such access details, access date and time and the operations performed during each session.
- **Operations:** View, add, modify and remove MSP administrative user accounts and the configuration of security policy settings.
 - **User Management:** MSP users help manage and maintain the MSP's Azara-powered, branded cloud service. Use the user management screens to manage MSP users.
 - **Security Policy Settings:** Use security policy settings to define parameters, such as maximum number of failed login attempts, password validity period, password length and *Two Factor Authentication* (2FA) to reduce threats to the network. These settings are applicable for all Tenants managed by the MSP.

Refer to the following sections:

- [Tenant Management](#)
 - [MSP Logs](#)
 - [MSP Operations](#)
-

1.1 Tenant Management

► *MSP Management*

Tenants are the MSP's end users who use the networks deployed across their sites to provide Azara Cloud services to their clients. Tenants in turn deploy cloud-managed networks consisting of one or more sites. Each site within the Tenant's network has access points deployed to provide clients with Azara Cloud service access. Once activated, Tenants can access their accounts and configure those parameters suiting their specific deployment objectives.

The *Tenants* tab lists existing Tenants created for this MSP account. Use this screen to view Tenant details, edit Tenants or add new Tenants.


Name	Email	Sites	Access Points	Access Point Down	License Expiry	Actions
Tenant_03	testing01@yah...	4	3	1	12/31/2017	
Tenant_02	testing02@yah...	1	1	1	12/31/2017	
KM	testing06@yah...	1	1	1	12/31/2017	
Tenant_04	testing05@yah...	0	0	0	12/31/2017	

Figure 1-1 MSP Account - Tenant tab

1. Review the following information for existing Tenants to assess whether a new Tenant requires creation or an existing account requires modification:

Name	Displays existing Tenants (active and disabled) created for this MSP account. Select a Tenant link to view the Tenant's Inventory/Devices screen and manage their devices (access points). Disabled Tenant accounts appear red.
Email	Displays the Tenant's e-mail address configured at the time of account creation.
Sites	Displays the number of sites configured within each Tenant. Select this link to view and manage the Tenant's <i>Site Details</i> .
Access Points	Displays the total number of access points added by each Tenant. Select this link to view and manage the Tenant's <i>Inventory/Devices</i> (access points).
Access Point Down	Displays the number of access points currently down (offline). Use this information to assess whether additional deployments are warranted to support client loads.
License Expiry	Displays the Tenant's current license status (<i>Active</i> or <i>Expired</i>) and the license expiry date. The license expiry date, for expired licenses, appears red. On license expiration, Tenants are allowed a 90 days license renewal grace period. During this time the Tenant's access point configurations remain unchanged. Once the grace period expires, the Tenant's access points revert to Factory Default settings, and all configuration tabs on the Tenant's account are disabled. However, the <i>License Info</i> tab remains enabled allowing the Tenant to apply new license.

<p>Actions</p>	<p>Displays icons for actions that can be performed on this Tenant account. The actions are editing the Tenant's detail or deleting the Tenant's account. Tenant accounts in red are disabled and cannot be edited. A Tenant account can be disabled for the following reasons:</p> <ul style="list-style-type: none"> • <i>If the account has not been activated by the tenant</i> - Two system-generated mails (containing the Azara Web link and the new Tenant's account password) are sent to the Tenant's registered e-mail address at the time of account creation. The Tenant is required to activate the new account by using this information to login to the Azara site, and changing the first-time login password. New Tenant accounts should be activated within 10 days from receipt of the above e-mails. If the account is not activated within the stipulated time frame, the account is automatically disabled. • <i>If the account has been deleted by the MSP</i> - Deleted Tenant accounts are not purged from the database and continue to appear in the MSP's Tenants list. Deleted accounts can be re-activated, if needed, at any time.
-----------------------	---

2. Select the  icon from the top right-hand corner to add a new Tenant. The following screen displays:

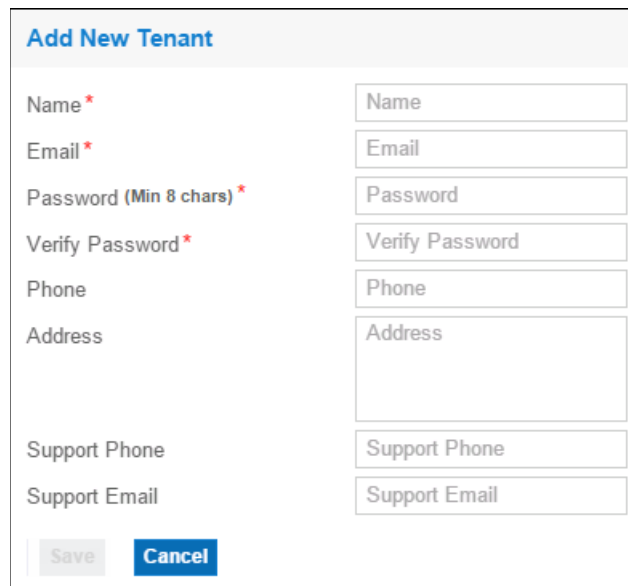



Figure 1-2 MSP Account - Add New Tenant screen

3. Enter the following to add a new Tenant configuration:

<p>Name</p>	<p>Enter the new Tenant's name. The name should be 2 - 32 characters. Special characters, such as underscore (_) and single quote (') are allowed. This field is mandatory.</p>
<p>Email</p>	<p>Enter the Tenant's e-mail address as an online contact resource. This field is mandatory.</p>
<p>Password (Min 8 chars)</p>	<p>Enter the password for this new Tenant account. Passwords must be between 8 - 12 characters long and contain at least 1 upper case character, 1 lower case character, 1 number and 1 symbol. This field is mandatory.</p>
<p>Verify Password</p>	<p>Re-enter the password to confirm it. This field is mandatory.</p>
<p>Phone</p>	<p>Enter the Tenant's contact phone number.</p>
<p>Address</p>	<p>Enter the Tenant's physical address as a mailing address contact resource.</p>

1-4 Azara MSP User's Guide

Support Phone	Enter the support contact number. This is the phone number of the MSP's support services. The Tenant, if necessary, can edit this information on account activation.
Support Email	Enter the support e-mail address. This is the e-mail address of the MSP's support service. The Tenant, if necessary, can edit this information on account activation.

4. Select **Save** to save the information and create the new Tenant configuration. Select **Cancel** to exit the *Add New Tenant* screen without saving the information.
5. To modify an existing Tenant, select the Tenant from amongst those listed and select the  icon. Tenant accounts in red are either not activated or are deleted and cannot be modified.

Edit Tenant

Name*

Email*

Phone

Address

Support Phone

Support Email

Figure 1-3 MSP Account - Edit Tenant screen


6. Edit all or any of the following information:

Name	Modify the Tenant's name as changes warrant.
Email	Modify the Tenant's e-mail address as contact information changes or becomes obsolete.
Phone	Modify the Tenant's contact number as needed to account for changes to contact information.
Address	Modify the Tenant's postal address to account for changes to the Tenant's mailing address.
Support Phone	Modify the support service's contact number as warranted by changes to contact information.
Support Email	Modify the support service's e-mail address as contact information changes warrant.

7. Select **Save** to save the modifications. Select **Cancel** to exit the *Edit Tenant* screen without saving the changes made to the Tenant's information.



NOTE: The **Save** button is enabled only if updates have been made to the original configuration.

8. To deactivate an existing Tenant, select the Tenant from amongst those available and select the  icon. A Tenant can be de-activated on expiry of license or lapse of subscription. To re-activate a Tenant, add a new Tenant, enter the de-activated Tenant's name and e-mail address, and click **Save**. On re-activation, all original settings for the Tenant are re-applied to the new account.



NOTE: A deactivated Tenant account will only be activated if the Tenant's name and e-mail id match with the inactive account. A new account will be created if the details do not match.

1.2 MSP Logs

► MSP Management

The *Logs* screen displays MSP user activity records. These records, also referred to as Audit logs, track customer activities and notify who has accessed the Azara site, the date and time of access, and the operations performed during that login session. The various user activities recorded are:

- Tenant/user login and logout details
- Network addition, deletion, and modification
- Site addition, deletion, and modification
- Inventory (access point) addition, deletion, and modification

Audit logs are chronologically arranged and troubleshoot and analyze network events. The pre and post event logs help identify an issue's root causes. Review these logs to identify account holders who are potential threats.

The following is a typical log screen.

Date/Time	Msp ↑	Tenant	User	Log Type	Log Message
08/23/2016 11:09:39	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	user_add	User (yaatirai-testing05@yahoo.com) was created with role as TENANT and accessType as ADMIN
08/23/2016 11:08:40	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	user_delete	User (yaatirai-testing05@yahoo.com) was deleted having role as TENANT and accessType as ADMIN
08/23/2016 11:07:30	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	user_add	User (yaatirai-testing06@yahoo.com) was created with role as TENANT and accessType as ADMIN
08/23/2016 10:54:30	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	login	Login Successful with IP 103.205.216.80
08/23/2016 10:40:20	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	logout	Logout
08/23/2016 10:33:42	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	login	Login Successful with IP 103.205.216.80
08/23/2016 09:46:36	TechPubs	RajeevKM	CSP(user_id :csp@zebra.com, As Role : csp)	tenant_to_csp	Back from Tenant: RajeevKM to CSP: CSP
08/23/2016 09:46:32	TechPubs	RajeevKM	CSP(user_id :csp@zebra.com, As Role : csp)	csp_to_tenant	From CSP: CSP to Tenant: RajeevKM
08/23/2016 09:45:36	TechPubs	Tenant_03	CSP(user_id :csp@zebra.com, As Role : csp)	tenant_to_csp	Back from Tenant: Tenant_03 to CSP: CSP
08/23/2016 09:45:31	TechPubs	Tenant_03	CSP(user_id :csp@zebra.com, As Role : csp)	csp_to_tenant	From CSP: CSP to Tenant: Tenant_03
08/23/2016 09:40:06	TechPubs	Tenant_03	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	msp_to_tenant	From MSP: TechPubs to Tenant: Tenant_03
08/23/2016 09:22:26	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	login	Login Successful with IP 140.101.148.1
08/22/2016 14:26:37	TechPubs	Tenant_03	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	msp_to_tenant	From MSP: TechPubs to Tenant: Tenant_03
08/22/2016 14:26:34	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	login	Login Successful with IP 140.101.148.1
08/22/2016 13:58:09	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	logout	Logout
08/22/2016 13:57:43	TechPubs	Tenant_03	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	msp_to_tenant	From MSP: TechPubs to Tenant: Tenant_03
08/22/2016 13:27:32	TechPubs	Tenant_03	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	msp_to_tenant	From MSP: TechPubs to Tenant: Tenant_03
08/22/2016 13:26:37	TechPubs	-	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	login	Login Successful with IP 140.101.148.2
08/22/2016 10:19:04	TechPubs	Tenant_03	TechPubs(user_id :tpq483@zebra.com, As Role : msp)	msp to tenant	From MSP: TechPubs to Tenant: Tenant_03

Figure 1-4 MSP Account - Logs screen

The following log information is displayed:

Date/Time	Displays the day and time when each listed log was generated. Use this date stamp to assess whether one or more log entries coincide with a particular network event requiring MSP administration.
MSP	Displays the logged MSP's name. For an MSP user, this column in the Audit Log remains unchanged and displays the MSP account name.
Tenant	Displays the logged Tenant's name. This column remains blank if the user is an MSP user and not a Tenant.
User	Displays the logged user's details, such as user ID, e-mail address and role.

Log Type	Displays the network activity used as log file creation criteria.
Log Message	Displays a system-generated event message. The message contains a brief description of the activity generating the log. For some log records, specifically, for configuration changes, a View diff link is displayed. Select the link to view further details about the activity generating the log and to identify the changes made to the configuration.

Log Details of HW Blv ⊗			
Updated Property Name	Old Value	New Value	Operation
map_coordinates	,	33.775673,-118.15118	UPDATE
country		United States	UPDATE
region		California	UPDATE
campus		Newport Avenue	UPDATE
city		Long Beach	UPDATE

Figure 1-5 MSP Account - Logs screen - Log Details screen

The *Log Details* screen displays the following information:

Updated Property Name	Lists the internal name for the property that was modified by this configuration change.
Old Value	Displays the old value before the change.
New Value	Displays the value after the change.
Operation	Displays the operation that was performed.

1.3 MSP Operations

▶ *MSP Management*

Use the *Operations* screens to configure various global settings for accounts managed by the MSP. Create and manage users, configure account lockout settings, password expiry settings, password history settings and login IP range restrictions.

Optionally enable or disable two factor authentication for Tenant accounts managed by this MSP.

Refer to the following sections:

- *MSP Users*
- *MSP Preferences*
- *Two Factor Authentication*

1.3.1 MSP Users

► *MSP Operations*

The *MSP Operations* tab opens the *Users* page by default. Use this page to manage (add, remove or modify) MSP users. MSP users manage and maintain the MSP's branded, Azara cloud service. MSPs can create multiple users with different levels of access permissions to suit their operational requirements.

Access permission is assigned when the MSP user account is created. The user's role within the Azara system is defined by the assigned access permission.

MSP users are categorized as:

- *Super Admin*: This account is created when the MSP account is created. There can only be one Super Admin account for the MSP account. This permission cannot be assigned to any other account.
- *Admin*: An MSP account can have multiple users with Admin permissions. The Super Admin user, upon account activation, can add the first Admin user. An Admin user can, in turn, add other Admin users, Read/Write users, and Read users.
- *Read/Write*: An MSP account can have multiple users with Read/Write permissions. Users with this permission can modify all configuration parameters.
- *Read*: An MSP account can have multiple users with Read permission. Users with this permission can only view configuration details. These users do not have write/modify permissions.



NOTE: Every MSP account has one Super Admin user, who is the first MSP user registered by the *Cloud Service Provider (CSP)* when creating the MSP account. E-mail verification and password mails are sent to the Super Admin's registered e-mail address. The MSP account is activated only after the e-mail verification process is successfully completed by the Super Admin. The MSP Super Admin can be added, deleted, or modified only by a CSP Super Admin.

MSP users have the following capabilities:

- Tenant account management (add, delete, edit and view Tenant accounts) - Super Admin, Admin, and Read/Write users. An MSP user can modify a Tenant account only if granted read-write permissions by the Tenant.
- Tenant subscription management
- MSP user account management (add, delete, edit, and view user accounts) - Super Admin, Admin, and Read/Write users
- Dashboard View - Super Admin, Admin, Read/Write users, and Read users

The following table lists the capabilities of the various MSP user roles:


MSP User Capabilities ↓	MSP Users →	Super Admin	Admin	Read-Write	Write
Can add, delete, edit, view an Admin User?	Add	Yes	Yes	No	No
	Delete	Yes	No	No	No
	Edit	Yes	Yes	No	No
	View	Yes	Yes	Yes	Yes
Can add, delete, edit, view a Read/Write User?	Add	Yes	Yes	Yes	No
	Delete	Yes	Yes	No	No
	Edit	Yes	Yes	Yes	No
	View	Yes	Yes	Yes	Yes

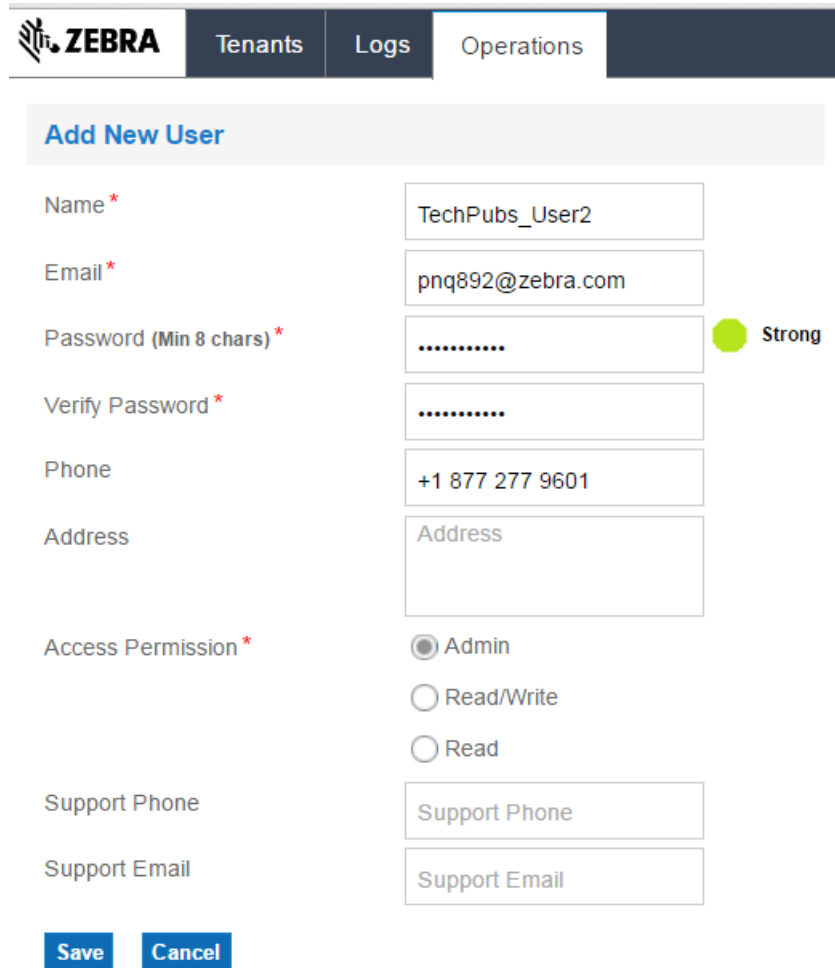
1-10 Azara MSP User's Guide

Can add, delete, edit, view a Write User ?	Add	Yes	Yes	Yes	No
	Delete	Yes	Yes	Yes	No
	Edit	Yes	Yes	Yes	No
	View	Yes	Yes	Yes	Yes
Can add, delete, edit, view a Tenant ?	Add	Yes	Yes	Yes	No
	Delete	Yes	Yes	Yes	No
	Edit	Yes	Yes	Yes	No
	View	Yes	Yes	Yes	Yes

1. Review the users configured for this MSP account.

Name	Displays the MSP user's name.
Email	Displays the MSP user's e-mail address, registered at the time of user account creation.
Phone Number	Displays the MSP user's phone number, configured at the time of user account creation.
Account Status	Displays the MSP user's account status. Displays <i>Active</i> when the account status is fine and in use currently.
Access Permission	Displays the MSP user's access permissions, assigned during user account creation. Access permissions include <i>Admin</i> , <i>Read/Write</i> , or <i>Read</i> .
Actions	Displays icons for the actions available on this MSP user account.

2. Select the  icon on the top, right-hand corner of the **User Details** bar to add a new MSP user.



ZEBRA Tenants Logs Operations

Add New User

Name* TechPubs_User2

Email* pnq892@zebra.com

Password (Min 8 chars)* Strong

Verify Password*

Phone +1 877 277 9601

Address Address

Access Permission* Admin
 Read/Write
 Read

Support Phone Support Phone

Support Email Support Email


Save Cancel

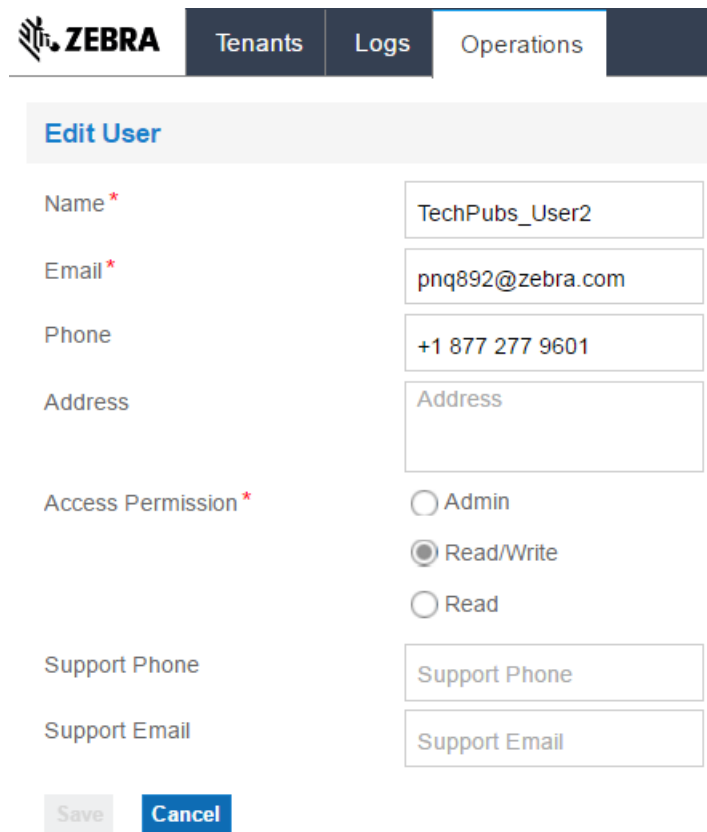
Figure 1-6 MSP Account - Operations - Add New User screen

3. Enter the following information to create a new user:

Name	Enter the new MSP user's name. The name should be 2 - 32 characters. Special characters, such as underscore (_) and single quote (') are allowed. This field is mandatory.
Email	Enter the MSP user's e-mail address. This field is mandatory.
Password (Min 8 chars)	Enter the password associated with this MSP user account. The password should be 8 - 12 characters and contain at least 1 upper case character, 1 lower case character, 1 number and 1 character symbol. This is a mandatory field.
Verify Password	Re-enter the password to confirm it. This is a mandatory field.
Phone	Enter the MSP user's contact number as a primary means of contacting the user quickly.
Address	Enter the MSP user's mailing address.
Access Permission	Select the access level for this MSP user. The options are: <i>Admin</i> , <i>Read/Write</i> and <i>Read</i> . This field is mandatory.

Support Phone	Enter an MSP account's support contact number. The new MSP user can use this number for troubleshooting issues encountered within the cloud network.
Support Email	Enter an account's support e-mail address. The new MSP user can use this e-mail address for troubleshooting.

4. Select **Save** to create the new MSP user. Select **Cancel** to exit the **Add New User** screen without saving the updates.
5. To modify an existing MSP user configuration, select the user account from amongst those listed and select the  icon. The following screen displays.



ZEBRA Tenants Logs Operations

Edit User

Name * TechPubs_User2

Email * pnq892@zebra.com

Phone +1 877 277 9601

Address Address

Access Permission * Admin Read/Write Read

Support Phone Support Phone

Support Email Support Email

Save Cancel


Figure 1-7 MSP Account - Operations - Edit User screen

6. Edit all or any of the following user information:

Name	Modify the name of the MSP user to accurately reflect the name change required.
Email	Modify the MSP user's e-mail address as it becomes obsolete for a specific user.
Phone	Modify the MSP user's contact number as their primary means of quick contact.
Address	Modify the MSP user's mailing address as their primary address changes.
Access Permission	Modify the MSP user's access permission. User roles and their permissions are specified in detail in the table listed earlier in this topic. Note: The access permission of the MSP Super Admin cannot be edited.
Support Phone	Update the support contact number provided when creating the MSP user if changes warrant new contact information.

Support Email

Modify the support e-mail address provided at the time of MSP user creation if their Internet contact credentials require update.

7. Select **Save** to save the edits or select **Cancel** to exit the **Edit User** screen without saving the changes.
8. To delete an existing MSP user, select the  icon located to the right of the user account to be deleted. A message is displayed asking for confirmation to delete the MSP user account.

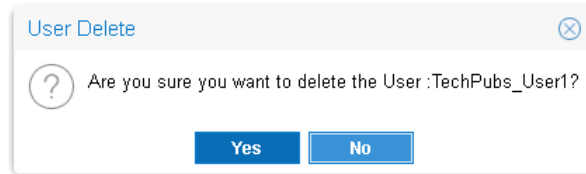


Figure 1-8 MSP Account - Operations - Delete User Confirmation screen

9. Select **Yes** to delete the MSP user. Select **No** to exit without deleting the MSP user.

1.3.2 MSP Preferences

► [MSP Operations](#)

Use the *Preferences* screen to configure the Security Policy applicable to the MSP's Tenants. MSP administrators have the option to lock out users after a defined number of failed login attempts, provide a time-frame on a passwords usage, restrict the number of times a password can be re-used, customize a password's length and add a second password attribute to reduce threats to the network.

1. From the **Operations** tab, select **Preferences**.

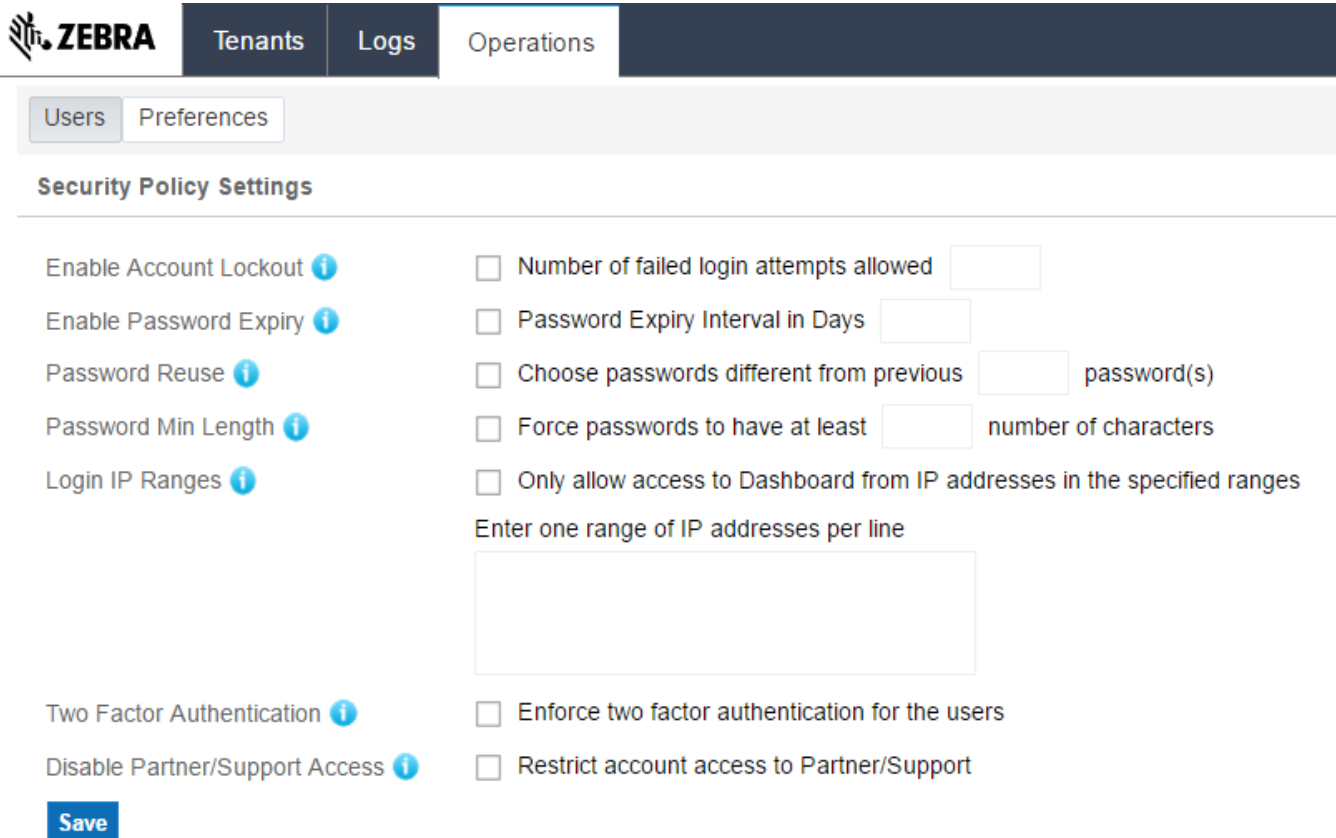


Figure 1-9 MSP Account - Operations - Preferences screen

2. Configure the following **Security Policy Settings** for the MSP account:



NOTE: Use the **i** icon to display a brief description for each of the fields in this screen.

<p>Enable Account Lockout</p>	<p>If selected, configure the maximum number of <i>failed</i> login attempts allowed before an account is locked. For example, if set to 3, the account is locked after 3 consecutive failed login attempts. The default value is 5 attempts. This option is disabled by default.</p>
<p>Enable Password Expiry</p>	<p>If selected, specify the password's validity period in days. For example, if set to 40 days the password remains valid for only 40 days from the date of creation and should be reset before expiration. The default value is 90 days. This option is disabled by default.</p>

Password Reuse	If selected, configure the number of previous passwords that <i>cannot</i> be reused. For example, if set to 3, the last three passwords cannot be re-used. The default value is set at 6 passwords. This option is disabled by default.
Password Min Length	This option forces a minimum length restriction on MSP user passwords. If selected, specify the minimum password length. For example, when set to 10, the password has to have a minimum of 10 characters. The default value is 8 characters. This option is disabled by default.
Login IP Ranges	If selected, provide the IP address(es) that can access the MSP dashboard. For example, if the range provided is 10.233.216.0/24, any IP address outside this range cannot access this MSP network. This option is disabled by default.
Two Factor Authentication	<p>This option enforces two factor authentication. <i>Two factor authentication (2FA)</i> enhances the network's security by requiring users to provide a second authentication value, such as a number or a phrase in addition to the account password. This second authentication value is delivered to the user's Extreme Networks-cloud verified mobile device.</p> <p>Once enforced on the MSP account, two factor authentication is applicable to the MSP's account users. On their first login attempt, post two factor authentication enforcement, users are prompted to complete the verification process. Two factor authentication enforcement is disabled by default.</p> <p>For more information on configuring two factor authentication, see <i>Two Factor Authentication on page 1-16</i>.</p>
Disable Partner/Support Access	Select this option to prevent the service provider (MSP) from accessing data on any tenant's network. When selected, at the MSP level, is applicable to all tenants of the MSP.

3. Select **Save** to save the Security Policy Settings and exit the screen.

1.3.3 Two Factor Authentication

▶ *MSP Operations*

Two Factor Authentication (2FA) provides a second and additional layer of security to your Azara account.

To access your account:

1. Navigate to the Azara login page and enter your Azara account login credentials.

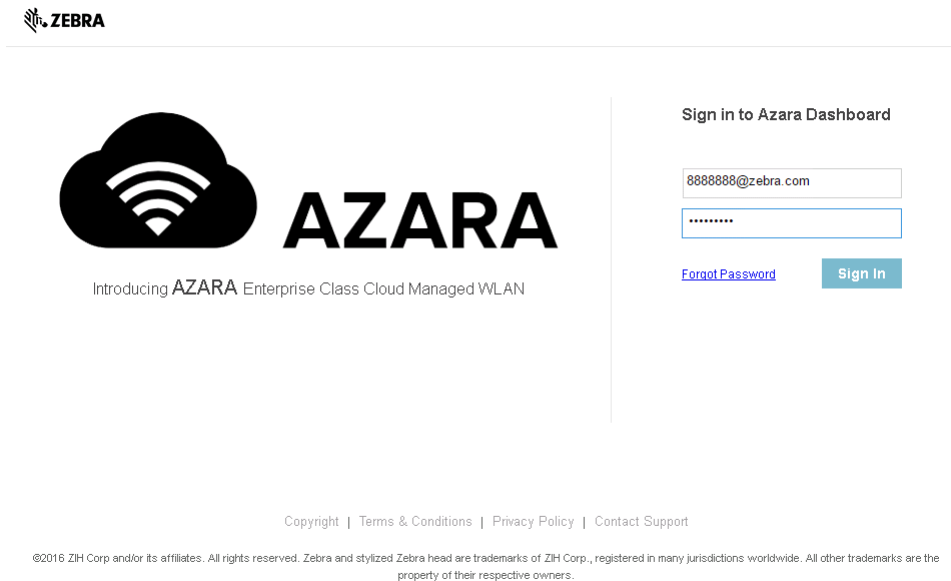


Figure 1-10 *MSP Account - Login screen*

2. Provide the time-based *Google Authenticator* verification code displayed on your mobile device. The Google Authenticator verification code is generated only if your Azara account is added to the Google Authenticator application on the mobile device used for two factor authentication.

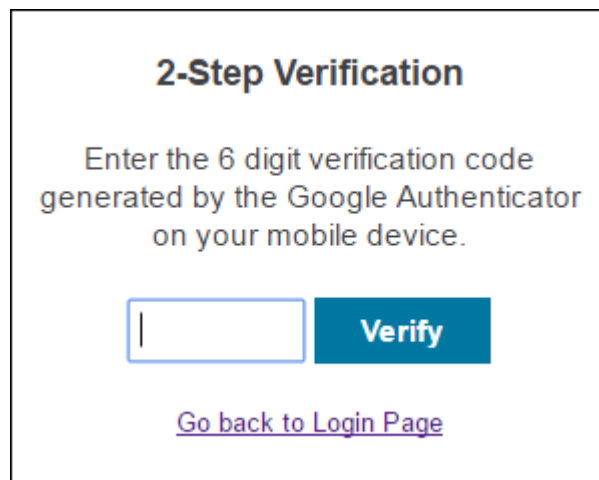


Figure 1-11 *MSP Account - Two Factor Authentication Code screen*

Two factor authentication mode is:

- enforced across the MSP account by the MSP Super Admin
- or
- enabled on an individual MSP account by the account holder

Enforcing two factor authentication across the MSP account

To enforce two factor authentication across the MSP account, navigate to the [Operations > Preferences](#) page, and select the [Enforce two factor authentication for the users](#) check box. You must have either *Super Admin* or *Admin* privileges to enforce this feature.



Two Factor Authentication 	<input type="checkbox"/> Enforce two factor authentication for the users
Disable Partner/Support Access 	<input type="checkbox"/> Restrict account access to Partner/Support
Save	

Figure 1-12 MSP Account - Two Factor Authentication Inheritance Across the MSP Account

When enforced on the MSP account, two factor authentication is automatically inherited by MSP users (existing and post-enforcement), Tenants (post-enforcement only) and Tenant end users. Two factor authentication mode is not enforced on Tenant accounts added prior to enforcement.



NOTE: A Tenant's Super Admin can disable two factor authentication enforcement at the Tenant account level. However, two factor authentication enforcement cannot be disabled by MSP users at their individual account levels.

Since the time-based Google Authenticator verification code is generated on the MSP user's registered mobile device, it is essential that you register (verify) your mobile device with Extreme Networks Azara cloud service. On your first login attempt - post two factor authentication enforcement - you are prompted to complete the registration process.

Select the [Set up Two Factor Authentication](#) link. The *Two Factor Authentication* page displays. Follow the instructions provided in the section *Registering your mobile device for Two Factor Authentication with the Azara cloud service on page 1-20*.

ZEBRA

Your account has been enforced to set up the two factor authentication. Complete the setup to login.


[Set up Two Factor Authentication](#)

Figure 1-13 MSP Account - Two Factor Authentication Inheritance Across the MSP Account



NOTE: If Two Factor Authentication is already setup on your mobile device, you are directly forwarded to the verification code page.

Enabling Two Factor Authentication on an individual MSP account

1. Login in to your Azara cloud account.
2. On the Title bar, click on the  icon displayed besides the **Welcome <ACCOUNT-NAME>** message, and select [Account Settings](#).

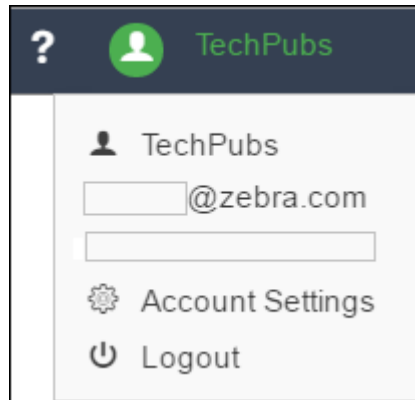


Figure 1-14 MSP Account - Account Settings option

The Account Settings screen displays.

A screenshot of the ZEBRA Account Settings page. The ZEBRA logo is in the top left. The page title is 'Account Settings' with a close button. The form contains: Name (TechPubs), Support Phone (+1 877 277 9231), Email ([redacted]@zebra.com), Support Email (Support Email), Address (Address), and Phone (Phone). There is a 'Change Password' link. Below the form are three expandable sections: 'Your Recent Logins', 'Your Active Sessions', and 'Two Factor Authentication Settings'. A 'Save' button is at the bottom left.

Figure 1-15 MSP Account - Account Settings screen

3. Expand the **Two Factor Authentication Settings** option.
4. Select the **ON** radio button. This option is disabled by default.

The *Two Factor Authentication* screen displays.

Two Factor Authentication Settings

Two Factor Authentication : OFF ON

Instructions for setting up Two Factor Authentication

- Install Google Authenticator on your Android Phone or iPhone
 - To use Google Authenticator on your Android device, it must be running Android version 2.1 or later
 - Downloading the app**
 - Visit Google Play
 - Search for **Google Authenticator**
 - Download and install the application
 - To use Google Authenticator on your iPhone, iPod Touch, or iPad, you must have iOS 5.0 or later. In addition, in order to set up the app on your iPhone using a QR code, you must have a 3G model or later
 - Downloading the app**
 - Visit the App Store
 - Search for **Google Authenticator**
 - Download and install the application
- Add your Zebra Cloud account to Google Authenticator using the **QR Code** or **Shared Secret** given below
- Record your one-time codes
- Verify your Device with Zebra Cloud by providing the time based one time password from your mobile
- Once your device is verified, save your changes using the Save Changes button

The QR Code for Two Factor Authentication of your account is :

The Shared Secret for Two Factor Authentication of your account is **pawe weah dqy6 4e3p v2lg iz4s hxi7 rnze** [Generate new Shared Secret](#)

Verify Your Device using the Time based One Time Password:

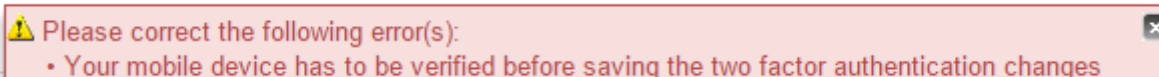
Verify

Note down the One-Time login codes for your account.

The One-Time codes for your account	
Code	Used
4cf4e3	false
c93d72	false
3e49c0	false
7d2864	false
67ccbb	false
cd6008	false
abea07	false
b6ca07	false
a20c83	false
d578a8	false

[Generate new set of One-Time codes](#)**Figure 1-16** MSP Account - Account Settings - Two Factor Authentication screen

If you select **Save**, without completing the registration process, you are prompted to verify your mobile device. The following message displays.

**Figure 1-17** MSP Account - Account Settings - Two Factor Authentication - Error Message

5. Complete the registration process described in the next section to verify your mobile device.



NOTE: The Azara cloud service uses the *QR code* or the *Shared Secret* displayed in the *Two Factor Authentication* page to verify your mobile device. Ensure this page remains open while registering your mobile device.

Registering your mobile device for Two Factor Authentication with the Azara cloud service

1. Open Google Authenticator on your Android phone or iPhone.

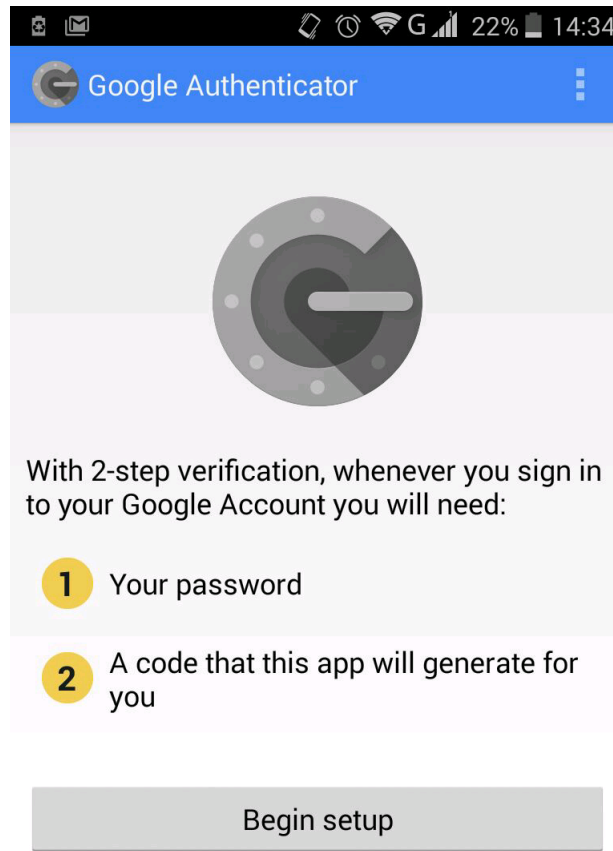


Figure 1-18 MSP Account - Two Factor Authentication - Open Google Authenticator

2. Select **Begin setup**. If setting up an account for the first time, the *Add an account* window opens by default. If adding a new Google Authenticator account, access the sub-menu and select *Set up account* option.

The Google Authenticator account associates the device with your Extreme Networks Azara cloud account. The time-based, Google Authenticator verification codes generated on your device under this account are required while accessing your Extreme Networks Azara cloud account. If necessary, create other accounts for securing similar services provided they support Google Authentication.

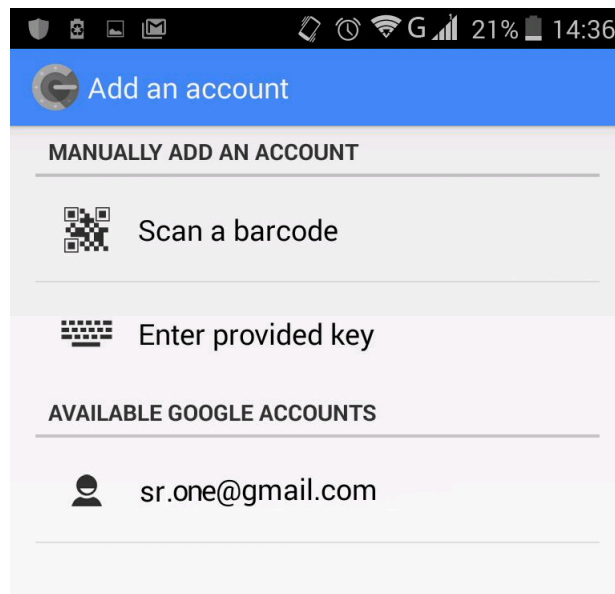


Figure 1-19 MSP Account - Two Factor Authentication - Add an Account screen

Accounts can be added to the Google Authentication application either by scanning a barcode or by entering a product key.

3. To add an account by scanning a bar code, use your mobile device to scan the QR code displayed under the Two Factor Authentication option.



NOTE: If you do not have a Barcode scanner installed on your mobile device, use the *Enter provided key* option for device verification and registration.

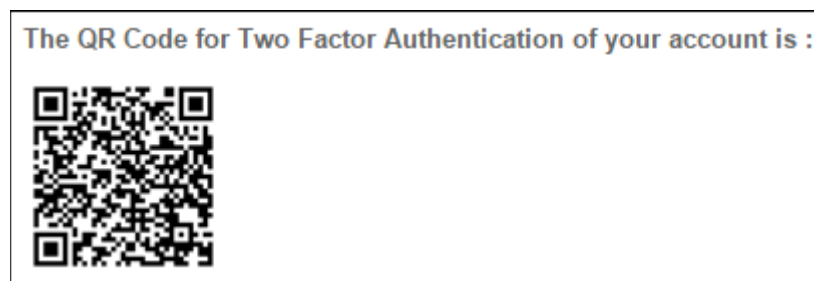


Figure 1-20 MSP Account - Two Factor Authentication - The QR Code

Once the QR Code is scanned successfully, the following message displays:

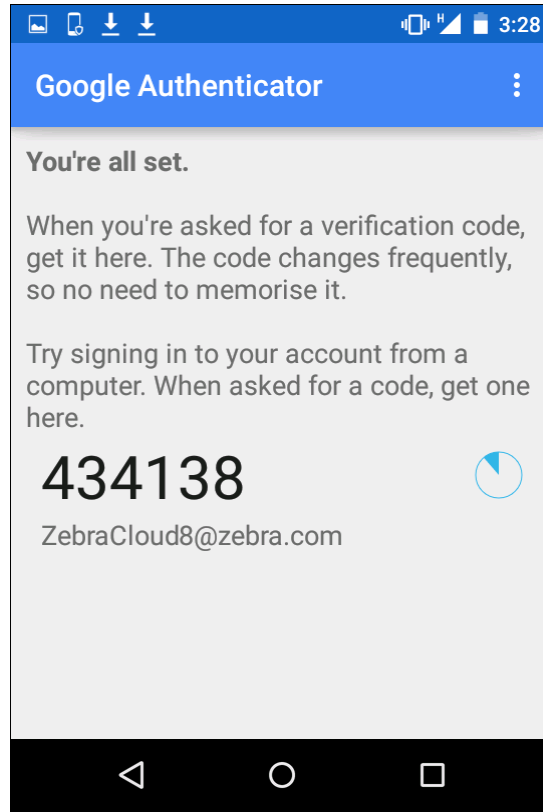


Figure 1-21 MSP Account - Two Factor Authentication - Account Verification Code

4. Enter the code displayed on your mobile's Google Authenticator application in the **Verify Your Device using the Time Based One Time Password** field.

Verify Your Device using the Time based One Time Password:	<input type="text" value="434138"/>	<input type="button" value="Verify"/>
---	-------------------------------------	---------------------------------------

Figure 1-22 MSP Account - Two Factor Authentication - Enter OTP

5. Click **Verify**. The following message displays upon successful device verification.

Two Factor Authentication Settings



Two Factor Authentication : OFF ON

Instructions for setting up Two Factor Authentication

- Install Google Authenticator on your Android Phone or iPhone
 - To use Google Authenticator on your Android device, it must be running Android version 2.1 or later
 - Downloading the app**
 - Visit Google Play
 - Search for **Google Authenticator**
 - Download and install the application
 - To use Google Authenticator on your iPhone, iPod Touch, or iPad, you must have iOS 5.0 or later. In addition, in order to set up the app on your iPhone using a QR code, you must have a 3G model or later
 - Downloading the app**
 - Visit the App Store
 - Search for **Google Authenticator**
 - Download and install the application
- Add your Zebra Cloud account to Google Authenticator using the **QR Code** or **Shared Secret** given below
- Record your one-time codes
- Verify your Device with Zebra Cloud by providing the time based one time password from your mobile
- Once your device is verified, save your changes using the Save Changes button

The QR Code for Two Factor Authentication of your account is :



The Shared Secret for Two Factor Authentication of your account is **pawe weah dqy6 4e3p v2lg iz4s hxi7 rnze** [Generate new Shared Secret](#)

Verify Your Device using the Time based One Time Password: ✔ Device verified successfully

Note down the One-Time login codes for your account.

The One-Time codes for your account	
Code	Used
4cf4e3	false
c93d72	false
3e49c0	false
7d2864	false
67ccbb	false
cd6008	false
abea07	false
b6ca07	false
a20c83	false
d578a8	false

[Generate new set of One-Time codes](#)

Figure 1-23 MSP Account - Two Factor Authentication - Device Verified Message

6. Click **Save** to update the settings. Click the icon to return to your account.
7. If using the **Enter provided key** option, the following Google Authenticator window displays on your mobile device.

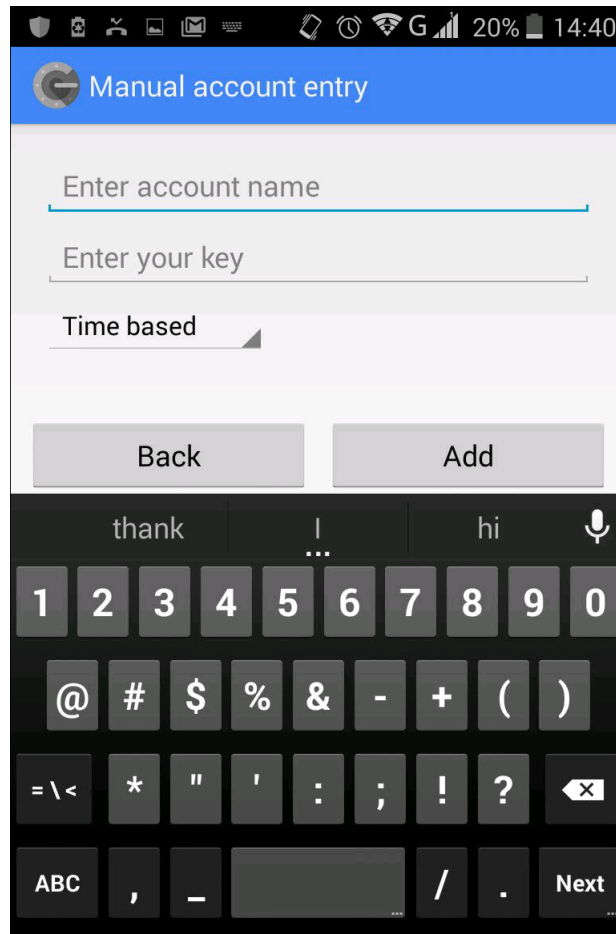


Figure 1-24 MSP Account - Two Factor Authentication - Provide a Key option

8. Enter an account name. This is the name of the Google Authenticator account created on your trusted mobile device. Provide a name for easy account identification for which this verification code applies.
9. Enter the key. This is the **Shared Secret** displayed under the Two Factor Authentication option on your Extreme Networks Azara cloud account. For example, the following image shows the shared secret as: **xk6n cyeg avrn xqav nqxl clge dcbl tqps**. Enter the code without the spaces.

The Shared Secret for Two Factor Authentication of your account is : **xk6n cyeg avrn xqav nqxl clge dcbl tqps** [Generate new Shared Secret](#)

Figure 1-25 MSP Account - Two Factor Authentication - Account Shared Secret

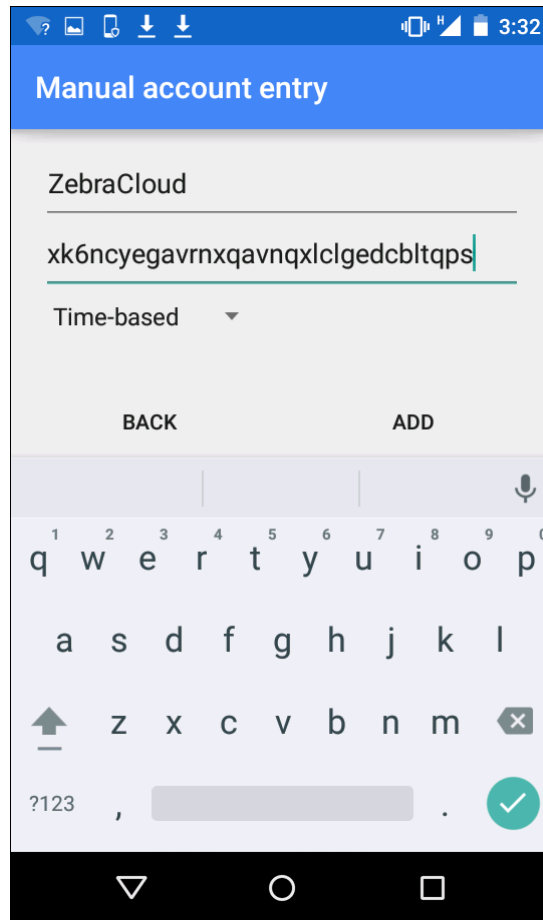


Figure 1-26 MSP Account - Two Factor Authentication - Enter Account Shared Secret

10. Click **ADD** on the Google Authenticator application. The following message displays upon successful verification:

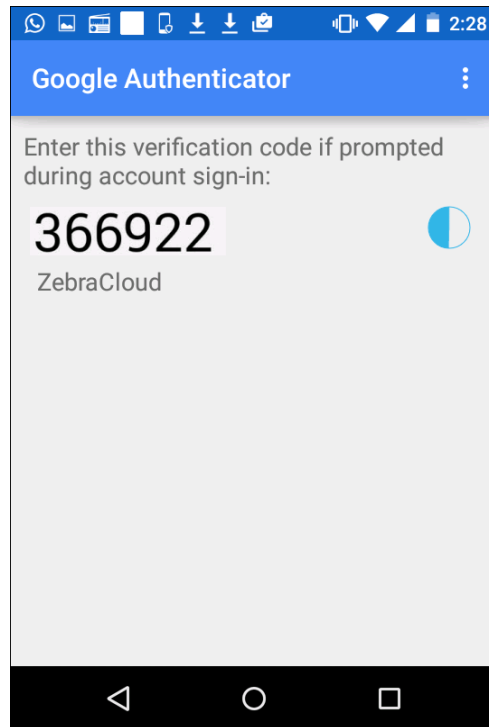


Figure 1-27 MSP Account - Two Factor Authentication - Account Login Verification Code

11. Enter the code displayed on your mobile's Google Authenticator application in the **Verify Your Device using the Time Based One Time Password** field.

Verify Your Device using the Time based One Time Password:

Figure 1-28 MSP Account - Two Factor Authentication - Enter Verification Code

12. Click **Verify**. A **Device verified successfully message** displays upon successful verification of your device.

Verify Your Device using the Time based One Time Password: ✓ Device verified successfully

Figure 1-29 MSP Account - Two Factor Authentication - Device Verified Successfully Message

13. Click **Save** to update the settings. Click the icon to return to your account.

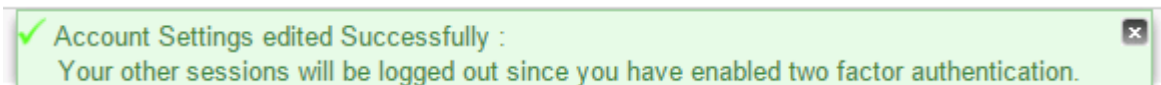


Figure 1-30 MSP Account - Two Factor Authentication - Account Settings Edited Successfully Message

14. Logout of your MSP account.

On subsequent logins, provide your Extreme Networks Azara credentials and the time-based Google Authenticator verification code on your mobile device.

1.3.3.1 Securing against loss of verified mobile device or deletion of Google Authenticator account

Each Two Factor Authentication supported MSP account has a set of ten, unique one-time codes. The codes are system generated when two factor authentication is enabled. The codes allow you to access your Extreme Networks Azara cloud account if you were to lose your verified mobile device or to delete the Google Authenticator account. Extreme Networks recommends retaining a copy of these one-time codes.

Note down the One-Time login codes for your account.

The One-Time codes for your account	
Code	Used
23172b	false
c9c631	false
4c3f3e	false
35e409	false
5b3cff	false
009270	false
7350ab	false
6ca000	false
11e572	false
413b15	false

[Generate new set of One-Time codes](#)

Figure 1-31 MSP Account - Two Factor Authentication - One-Time Account Login Codes

1. If unable to provide the verification code sent to your mobile device when logging in, enter any of the one-time codes as an alternative.

2-Step Verification

Enter the 6 digit verification code generated by the Google Authenticator on your mobile device.

[Go back to Login Page](#)

Figure 1-32 MSP Account - Two Factor Authentication - Entering One-Time Account Login Code

The following message displays upon successful verification of the one-time code:

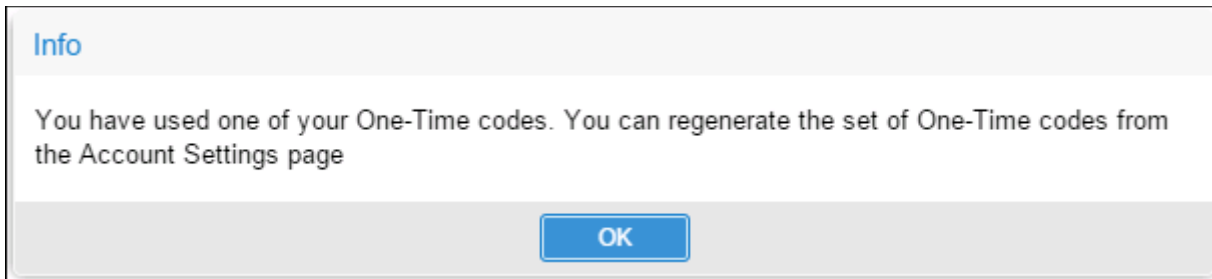


Figure 1-33 MSP Account - Two Factor Authentication - Regenerate One-Time Account Login Code Message

2. Click **OK** to proceed to your Extreme Networks Azara cloud account.
3. From inside your Azara account, navigate to the *Account Settings* page and expand the *Two Factor Authentication Settings* option. The status of the used one-time code appears as *true*. Once you have used all your available one-time codes, click the **Generate new set One-Time codes** link to generate a new set of ten, unique codes for your account. Retain a copy of these codes for future use.

Note down the One-Time login codes for your account.

The One-Time codes for your account	
Code	Used
23172b	true
c9c631	false
4c3f3e	false
35e409	false
5b3cff	false
009270	false
7350ab	false
6ca000	false
11e572	false
413b15	false

[Generate new set of One-Time codes](#)

Figure 1-34 MSP Account - Two Factor Authentication - New Set of One-Time Account Login Codes

APPENDIX A CUSTOMER SUPPORT

Customer Support

Customer support can be obtained through e-mail or through telephone within the time limits set forth in the support agreements.

When contacting customer support, please provide the following information:

- *Company Name*
- *Contact First and Last Name*
- *Contact Phone Number*
- *Contact E-mail*
- *Contact Mailing Address*
- *Azara Account Number*
- *Problem Description*

Support for Azara is available 24/7, 365 days a year only after the tenant account has been provisioned for the first time. Also, a customer must have an active Azara account for us to provide technical support via phone or e-mail.

Customer Support Through Phone

Azara customer support phone numbers are:

- Within the US: **1-800-653-5350**
- Outside the US: **011-302-444-9700**

Standard Support hours for North America are 8:00 AM to 8:00 PM Eastern. Support during Standard Support hours is available in **English** and **Spanish**.

After Support hours for North America are 8:00 PM to 8:00AM Eastern. Support during After Support hours is available in **English** only.

Extreme Networks's technical support representative will open a support request and begin steps to resolve the issue.

Customer Support Through E-mail

Azara customer support through e-mail is available through your Azara account. To obtain support via e-mail, login to your Azara web interface and click the **Contact Us** e-mail icon located in the top right corner of the user interface.

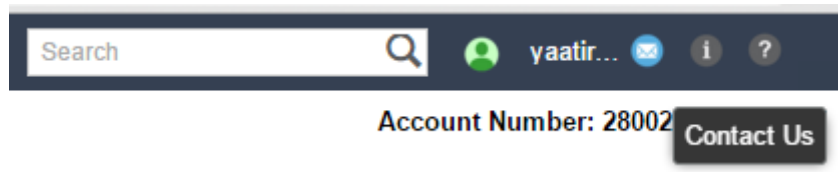


Figure A-1 *Contact Us Via Email*

Fill up the form, and if required, attach any documents and send.

Extreme Networks' technical support representative will open a support request and begin steps to resolve the issue.

