White Paper

Disaster Recovery Deployment Guide

V1.3

Contents

Introduction

This guide provides an overview of the Zscaler Disaster Recovery (DR) functionality, considerations for activation, feature constraints, and includes detailed step-by-step configuration activities needed to configure, activate, test, and recover from a incident. In addition, the document provides links to relevant help articles, which provide additional detail and configuration options.

About Disaster Recovery

The Zscaler Cloud offers flexibility, scalability, and security for users accessing applications from anywhere through a robust cloud infrastructure with regional redundancy, core infrastructure standbys, operational drills, and procedure planning. Zscaler has a long history of near-perfect uptime backed by best-in-class service-level agreements. However, a resilient solution must operate under black swan events where the cloud is not accessible due to natural disasters, technical failures, and human error.

With Zscaler DR, organizations can quickly restore access to Mission Critical Applications, even in events when the Zscaler Cloud is not available. The customer can initiate DR mode according to its Business Continuity plan to ensure current users continue accessing essential business applications. Once the event is over, the customer can restore the regular operation of the platform.

Disaster Recovery Prerequisites and Considerations

The underlying assumption during Disaster Recovery mode is that even though the Zscaler Cloud is not available, the customer's underlying infrastructure services remain operational. However, DR prerequisites, configurations, and infrastructure components must be in place before a Disaster Event. In addition, features and protections that rely on communication with the Zscaler Cloud services will be disabled tenant-wide while DR mode remains active and selectively during DR test mode.

DR for ZPA applications is enabled at the Application Segment Level. Zscaler recommends moving non-mission critical or risky applications under DR to new application segments.

Disaster Recovery has three operation modes:

- **Off:** Normal operations, ZPA Private Service Edge (PSE), App Connectors, and Zscaler Client Connector (ZCC) operate in cloud mode.
- **On:** DR Mode active. Only currently enrolled and authenticated users can access mission critical applications within application segments marked for DR through App Connectors and PSEs configured for DR.
- **Test:** Test Mode, used for testing DR Mode by applying DR to a group of users.

Platform Prerequisites

The prerequisites listed below are known to be applicable at the time of publication. For the latest information, review the “Understanding Disaster Recovery” article.

Platform prerequisites	
Item	Description
DNS Records	Ability to create a separate domain, TXT, and A DNS record for disaster recovery.
ZCC Versions	Windows 4.0 and above. MacOS 3.7.1.38 and above.
ZCC prerequisites	
Network Connectivity	End User devices must be able to reach DNS to resolve the Disaster Recovery domain. ZCC must be able to access the Zscaler-provider global database allow list. ZCC must be able to reach the ZPA Private Service Edges.
ZIA prerequisites	
Custom PAC File	The Custom PAC file must be reachable by HTTP or HTTPS when the ZIA service is unavailable.
ZPA prerequisites	
PSE and App Connector	Use the latest ZPA PSE and App Connector release.
DNS Records	DNS A records configured with the public IP of PSES enabled for DR.
Data Residency	Data Residency requirements should be documented and considered during DR Planning

Table 1 Disaster Recovery prerequisites

Unavailable Features during Disaster Recovery

The following information was current at the time of publication, for the latest information, review the article named “Understanding Disaster Recovery.”

Unavailable Platform Features	
Feature	Description
Authentication and enrollment	Only devices enrolled and authenticated users will be able to use ZIA, and ZPA
Reauthentication	Users who log out of ZCC will not be able to reauthenticate until DR Mode is disabled. The Zscaler SAML assertion validity is extended by 14 days(configurable in the ZPA UI) from the date the SAML assertion was issued when DR is activated.
Configuration Changes	Configuration changes (App Profiles, Policies, Zscaler hosted PAC files) will not be available.
Log Streaming Service	Logging during DR is unavailable at the time; engage with Zscaler Professional Services for additional information.
Source IP Anchoring Applications (SIPA)	SIPA applications are not available during DR at this time **
Data Protection	DLP, Filetype Control, Firewall, Sandbox, SSL Inspection, and Threat Protection are disabled
Unavailable ZIA Capabilities during DR Mode	
ZIA Policies	Global Traffic Forwarding Action applies (Send Traffic, Disable Traffic, Predefined-Traffic)

Unavailable Platform Features	
Web Security	Malware Protection, Advanced Threat Protection, Secure Browsing
Web Access Control	URL & Cloud App Control, Bandwidth Control
Firewall Filtering	DNS, FTP, IPS, and Forwarding Control
Unavailable ZPA Capabilities during DR Mode	
ZPA Policies	ZPA Policies are unavailable during DR Mode.
Portals and Browser Access	Privileged Remote Access Portal, User Portals, Browser Access are unavailable.
Connector Management	Branch and Cloud Connectors are unavailable during DR.
App Connector and PSE Enrollments	The infrastructure necessary to support users during DR must be deployed and online before the DR Event.
Machine Tunnels	Users without authenticated cached credentials and a network path to authentication infrastructure may be unable to login

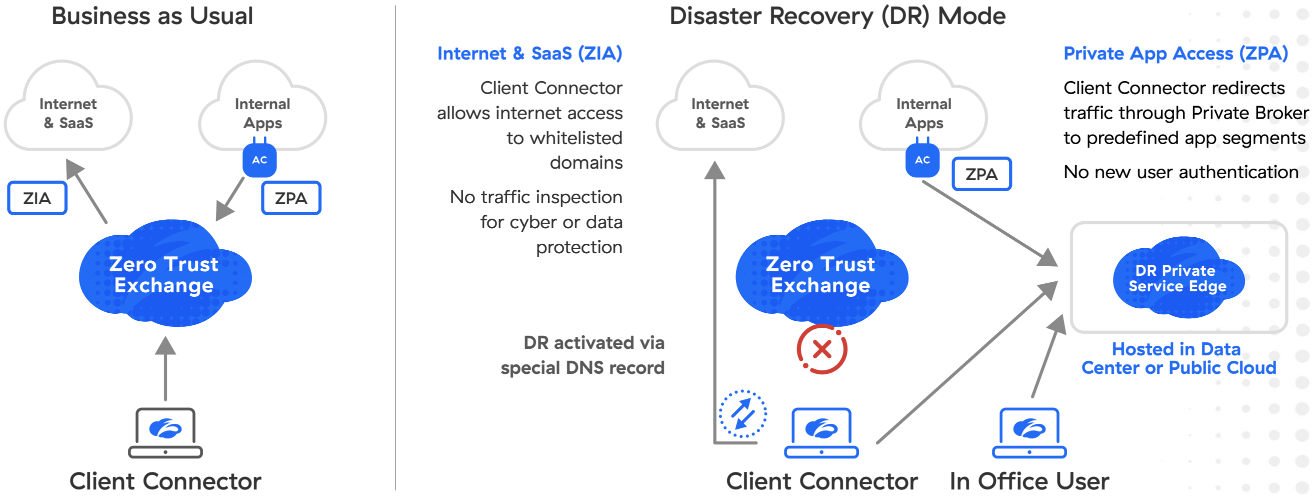
Table 2 Unavailable Features during DR Mode

** SIPA is available under specific configurations. SIPA Applications within a DR-enabled App Segment, App Connector, and PSE may be available during DR. The customer is encouraged to test their SIPA deployment using DR Test Mode. For additional information, please contact the Professional Services team.

Zscaler Disaster Recovery Architecture

Zscaler DR features aim to enable existing authenticated users and network-level access to mission critical applications identified in the customer's Business Continuity Plan. Mission critical Applications are those essential applications of suites of applications required by the business to operate effectively.

The underlying assumption for DR mode is that the Zscaler cloud is unavailable. Therefore, Zscaler utilizes DNS as an external service to initiate DR Mode. As such, the customer must register a domain name for disaster recovery and create a set of DNS A and specific TXT records. To simplify the creation of the DNS TXT records, Zscaler provides the Zscaler Record Generation tool. Review the DNS Configuration Section for details.


Business as Usual
Internet & SaaS
Internal Apps
AC
ZIA
ZPA
Zero Trust Exchange
Client Connector
Disaster Recovery (DR) Mode
Internet & SaaS (ZIA)
Client Connector allows internet access to whitelisted domains
No traffic inspection for cyber or data protection
DR activated via special DNS record
Internet & SaaS
Internal Apps
AC
ZPA
Zero Trust Exchange
Private App Access (ZPA)
Client Connector redirects traffic through Private Broker to predefined app segments
No new user authentication
DR Private Service Edge
Hosted in Data Center or Public Cloud
Client Connector
In Office User

Zscaler Internet Access (ZIA)
ZIA utilizes ZCC to protect web users' traffic by forwarding user traffic to the Zscaler service ensuring that access policies are enforced. In addition to protecting users during normal operation, ZCC downloads the Zscaler pre-defined global allow list** every 24 hours. It also queries the DNS service periodically to determine if DR mode is activated. When ZCC detects that DR is activated, it displays a "Safe Mode" notification popup, adds "Safe Mode" to the ZCC GUI, and creates notification log entries indicating that Internet Security Safe Mode has started.

ZIA DR provides three different traffic forwarding actions configured through App Profiles within the ZCC Portal. Zscaler recommends using the Allow Traffic to pre-selected destinations traffic action to continue providing internet access to whitelisted and known destinations. Review the ZIA Configuration section for details. Alternatively, customers can bypass all internet traffic through direct internet access or disable access altogether, depending on the company's risk tolerance. Review the article "About Disaster Recovery" for details on the three forwarding actions.

NOTE: Zscaler recommends reviewing all explicit bypass policies and mission critical destinations against the Zscaler pre-defined allow list. Add any missing locations to the Custom PAC file; otherwise, users won't get access to applications with DR Mode activated.

Zscaler Private Access (ZPA)
ZPA DR modes leverage the existing ZPA Infrastructure (App Connectors and ZPA Private Service Edges) to provide network-level access to mission critical applications and uses DNS to activate and deactivate DR Mode.

The ZPA Private Service Edge (PSE) manages connections between ZCC and App Connectors. During regular operation, the PSE and App Connectors download the relevant configurations from the ZPA Cloud. The App Connectors, in turn, provide the secure authenticated interface between a customer's servers and the ZPA cloud and are usually co-located as close as possible to the enterprise applications. For a detailed description of PSEs and App Connectors, review the "About ZPA Private Service Edges" and "About App Connectors" help articles at https://help.zscaler.com.

The ZPA components query DNS periodically to determine if DR mode is active by the contents of the TXT record. Once DR is activated, the following actions occur:

- The Zscaler SAML assertion validity is extended by 14 days to prevent users from losing access to DR applications when they reach a timeout. The value can be configured in Disaster Recovery Settings in the ZPA Admin Portal
- App Connectors and PSEs enabled for DR will reboot to enter DR mode.
- ZCC will resolve the disaster recovery domain A record and connect to the PSE behind the resolved IP.
- ZCC downloads the DR apps listed in the local configuration file of the PSE.
- ZCC forwards the mtunnels for the DR Apps to the PSE to provide network-level access to the applications.

Review the ZPA Disaster Recovery Configuration section for configuration details for the ZCC Portal, App Connectors, and PSE.

During the instantiation of DR mode, the user may become briefly disconnected from their applications. When DR is fully operational, users can only use mission critical applications enabled for DR.

Planning

Enabling Disaster Recovery has several implications for business operations depending on enabled product features. Therefore, the decision criteria for activation must be documented and integrated into customers' existing Business Continuity Plan. Consider the following factors when creating the plan.

- **Application Selection.** DR is enabled at the Application Segment level. To control mission critical applications for DR only, Zscaler recommends creating new application segments with only the desired applications. Non-mission critical applications should not be part of the group.
- **Situation assessment.** Ensure the situation is classified as a disaster, based on business impact (users/locations impacted, loss of productivity), restoration times, and impact of operating under reduced risk controls (unavailable features).

  Customers should utilize Zscaler's Trust Center as a data point to determine if a DR event should be activated. Trust Center provides the status of Zscaler's Cloud Services, including maintenance schedules, incidents, and advisories.
- **Restoration time.** Consider the expected resolution time for the outage versus the business risk of not activating Disaster Recovery. Disaster Recovery activation/restoration has a dependency on DNS propagation time. Consider the result of DR Activation / Restoration tests in the decision process.
- **Communication plan.** Ensure a clear communication plan outlines how the information will be shared with all relevant stakeholders, including employees, customers, vendors, and partners. The communication plan should define what applications will continue to be operational during Disaster Recovery.
- **Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).** Validate that the recovery time and data loss objectives specified in the disaster recovery plan are relevant, contain steps that include Zscaler services, and are achievable given the specific circumstances of the event.
- **Resource availability.** Ensure access to the necessary resources such as networking team, DNS administration, Networking, and Applications to activate and execute the disaster recovery plan.
- **Data Residency requirements.** DR-enabled PSEs should meet data requirements during DR, adjust the infrastructure, or document the risk as required.

Each organization may have additional decision criteria for activating a Disaster Recovery Plan. Zscaler recommends engaging with the appropriate teams to incorporate the Zscaler infrastructure and DR activities.

ZPA DR Infrastructure Capacity

ZPA DR Mode relies on PSEs and App Connectors to provide network-level access to mission critical applications during a DR event. During normal operations, PSEs and App Connectors can be added to the ZPA Service Groups anytime. Deploy enough App Connectors and PSEs capable of handling capacity during a DR Event before the event. Adding additional devices for scale during DR Mode is not possible. DR devices must be online before activating DR.

App Connector Capacity Planning

App Connectors provide the secure authenticated interface between a customer's applications and the ZPA cloud and are usually co-located with the enterprise applications with connectivity to the PSE. Review the document "About App Connectors." for the latest information. The number of App Connectors required is based on the aggregate throughput and the number of applications enabled for the Double Encryption feature. For a detailed understanding of throughput, please review the "Understanding App Connector Throughput" article.

At the time of publication, the following were the recommended sizing requirements for most platforms. For the latest information, review the article "App Connector Deployment Prerequisites" and the appropriate deployment guide for your platform located at https://help.zscaler.com/zpa/app-connector-management/app-connector-deployment-guides-supported-platforms.

Spec	Recommended Value
Memory	8 GB of RAM
CPU	2 CPU cores(Xeon E5 class) for physical machines without hyperthreading 4 CPU for virtual machines with hyperthreading
Disk Space	16 GB thin provisioned
Network Cards	2 NICs configured in a bonded pair
Max Aggregate throughput	500 Mbps per App Connector

Table 6 App Connector Recommended Specifications

Zscaler recommends deploying a larger quantity of App Connectors with lower specifications rather than fewer App Connectors with higher specifications to scale horizontally in an N+1 configuration where N is the number of App Connectors required per the sizing requirements. DR mode does not require dedicated infrastructure for operation if the infrastructure is properly sized to include both DR and DR Testing events, refer to the DR testing section for additional details.

ZPA Private Service Edge Capacity Planning

The quantity of PSEs used in an environment is determined by throughput and number of users connecting to ZPA. The following specifications were accurate at the time of publication, please reference the help article "ZPA Private Service Edge Deployment Prerequisites" for the latest information. Platform-specific deployment guides can be found in the "Private Service Edge Deployment Guides for Supported Platforms" article.

For a comprehensive guide on deploying ZPA Private Service Edges review the "Private Service Edge Management" section at https://help.zscaler.com/zpa/private-service-edge-management.

Spec	Recommended Value
Memory	8 GB of RAM for up to 2,000 connected users. Add 1 GB for every additional 1,000 active connected users
CPU	4 CPU cores(Xeon E5 class) for physical machines without hyperthreading 4 CPU for virtual machines with hyperthreading
Disk Space	16 GB thin provisioned
Network Cards	2 NICs configured in a bonded pair
Max Aggregate throughput	500 Mbps per App Connector

Table 7 PSE Recommended Specifications

ZPA Private Service Edges are designed to scale elastically. To support the total throughput required for DR Mode,add additional ZPA Private Service Edges to the appropriate ZPA Private Service Edge group using the corresponding Provisioning Key. Zscaler recommends deploying ZPA Private Service Edges in pairs (N+1), where N is the number of ZPA Private Service Edges as per the sizing requirements. DR mode does not require dedicated infrastructure for operation if the infrastructure is sized properly to include additional capacity for both DR and DR Testing events; refer to the DR Testing section for additional details.

NOTE: Plan for Scalability. App Connectors and PSEs capable of scaling to support user and application capacity during a DR event must be completed prior to the DR event. Adding additional devices during DR Mode is not possible. DR devices must be online before activating DR.

Disaster Recovery Configuration

Perform DR configuration after identifying mission critical applications and site destinations, assessing App Connector and PSE Capacity, reviewing considerations with the company's DR and Security Teams, and deploying any required additional infrastructure.

This section covers Zscaler 's recommended settings and provides an overview of the configuration. For detailed configuration, review the ZIA Disaster Recovery article at https://help.zscaler.com.

The high-level steps for DR configuration are listed below:

1. Configuration of DNS disaster recovery domain and DNS TXT records.
2. Enabling DR features for ZPA and ZIA for each App Profile in the ZCC portal.
3. Configuration Traffic Forwarding Actions for ZIA.
4. Enabling DR for mission critical Application Segments, App Connectors, and PSEs.

DNS Configuration

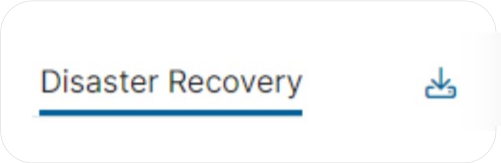
Disaster Recovery Mode is controlled by the disaster recovery domain DNS TXT record tags. DR can be triggered upon uploading the TXT record or scheduled using the start and end time parameters.

The DNS TXT records follow a format analogous to the Domain Key Identified Mail (DKIM) format. For a comprehensive description of the various parameters and tags available, review the article "Creating DNS TXT Records." Zscaler recommends using signed DNS TXT records; unsigned DNS TXT records for DR operations due to the additional controls required. Unsigned DNS TXT records are also available.

Although the DNS TXT records can be created manually, Zscaler recommends using the Zscaler DNS Record Generator tool to ensure proper syntax and sign the records. At the time of publication, the tool is only supported for Windows OS Devices and must be run as an administrator. For the latest information and installation details, review the article "About the Zscaler DNS Record Generator."

1. **Select and register a Disaster Recovery Domain.** Choose or create a new domain dedicated to DR. The same domain name can be used for ZIA and ZPA and will be entered in the ZCC and ZPA Admin portals.

2. **Download the Zscaler DNS Record Generation tool.** In the ZPA Admin Portal, navigate to Administration –> Settings –> Disaster Recovery and click the download icon



3. **Install the Zscaler DNS Record Generation tool.** Use this tool to create the DNS TXT records and the signature Disaster Recovery Key Pairs.

4. **Create key pairs.** If keypairs have not been created, use the Zscaler Record Generator tool to create keypairs and store them according to the company's security policy.

5. **Generate Signed DNS TXT Records.** Create the signed DNS TXT Records with the following settings:

Generator Tool Prompt	Value	Notes
Signed DNS records?	Yes	Zscaler recommends only using signed records to perform DR operations.
Create a key pair?	Yes	The Zscaler tool will generate a 2048-bit RSA key pair necessary for signing operations, files are saved in the /Files folder within the install directory named: dr_privatekey.pem and dr_publickey.pem Care must be taken to secure the private key according to company policy.
Disaster Recovery needs to be configured for ZIA?	Yes	If activating DR for ZIA, otherwise set No
Overwrite ZCC Portal configuration	No	Zscaler recommends using the Pre-defined Destinations option that is only configured in ZCC Portal

Generator Tool Prompt	Value	Notes
Disaster Recovery needs to be configured for ZPA	Yes	If activating DR for ZPA, otherwise set to No
Set the disaster recovery status for the disaster recovery domain;	On	Enable DR Mode, other options are Off to deactivate Disaster Recovery and Test to activate DR Test Mode
Do you want to start disaster recovery now?	Yes	Setting the value to Yes will activate DR mode once the DNS TXT record is uploaded and DNS propagates. To schedule, DR activation set the value to No and enter the date of the activation in yyyy-mm-dd format and time in UTC using the hh-mm-ss format
Default disaster recovery activation ? (runtime = 7 days)	Yes	By default DR remains active for 7 days from the start time. To schedule an end time
Default disaster recovery activation? (custom duration)	No	Enter the date for deactivation in yyyy-mm-dd format and time in UTC using the hh-mm-ss format

Table 8 Zscaler DNS Record Generator Tool values for initial configuration

6. **DNS TXT Records.** The DNS TXT records will be stored in the /Files folder within the Zscaler Record Generator Tool program folder. Uploading the DNS TXT record to DNS will perform the action configured in the tool.

7. **ZPA DNS A Records.** DR-enabled PSEs must be publicly accessible and reachable by the ZCC. Each publicly accessible DR-enabled PSEs, requires a DNS A record created within the customer environment. During Disaster Recovery mode, ZCC relies on DNS resolution to determine which PSE it will connect. Refer to the customer's DNS provider to determine how to implement Global Server Load Balancing if PSE selection by round-robin is unsuitable for deployment.

ZIA Configuration

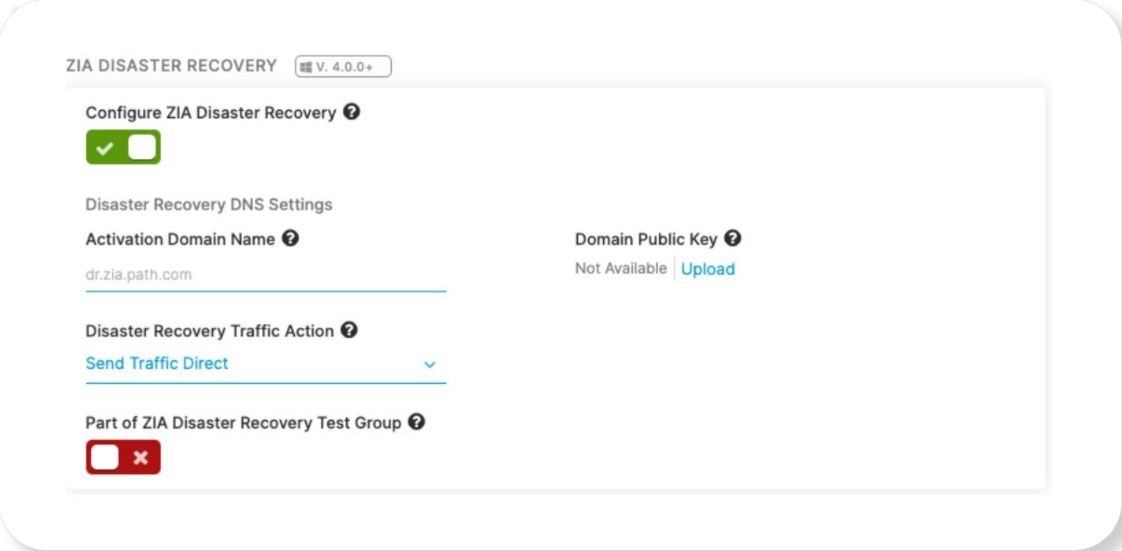
DR mode for ZIA allows enrolled users to continue accessing internet applications when the ZIA service is not available, based on the Traffic Forwarding Action. Configure the Traffic Forwarding Action in the App Profiles section within the ZCC Portal:

1. In the ZIA Admin Portal, go to Policy -> Zscaler Client Connector Portal

2. Click App Profiles

3. For each supported platform (Windows and macOS), edit an existing policy or create a new one as applicable.

4. Scroll down to the ZIA Disaster Recovery Section and toggle Disaster Recovery service



ZIA DISASTER RECOVERY V. 4.0.0+

Configure ZIA Disaster Recovery ☑

Disaster Recovery DNS Settings

Activation Domain Name: dr.zia.path.com

Domain Public Key: Not Available | Upload

Disaster Recovery Traffic Action: Send Traffic Direct

Part of ZIA Disaster Recovery Test Group ☒

5. Configure ZIA Disaster Recovery Settings

Setting	Input Description
Activation Domain Name	Enter the disaster recovery domain name
Domain Public Key	Upload the dr_publickey.pem file created with the Zscaler Record Generator Tool. This key is used to validate the DNS TXT records
Disaster Recovery Traffic Action	Zscaler Recommends using the Pre-Selected Destinations option along with Use Zscaler Pre-Selected Destinations and Use Custom Destinations. The Zscaler Pre-Selected Destination list contains whitelisted URLs; review the article “About Disaster Recovery” for the current list location. Enter the URL (including the http or https prefix) for a custom PAC file not hosted in Zscaler. The Custom PAC file should include three types of domains: • External mission critical domains not included in the Global Allow list. • All the bypassed domains not contained in Zscaler’s pre-selected destination list. • Domains included in Zscaler’s Global Allow list that the customer wishes to explicitly block For custom PAC file examples, review the Traffic Forwarding Section in the document titled “About Disaster Recovery at https://help.zscaler.com. The Send Traffic option bypasses ZCC, allowing the user access to any destination through direct internet access. Disable Internet Traffic will cause all traffic to drop at the endpoint, preventing internet access to ZCC users.
Part of ZIA Disaster Recovery Test Group	Zscaler recommends having at least one profile per platform designated as a DR Test Group with a corresponding group of test users.

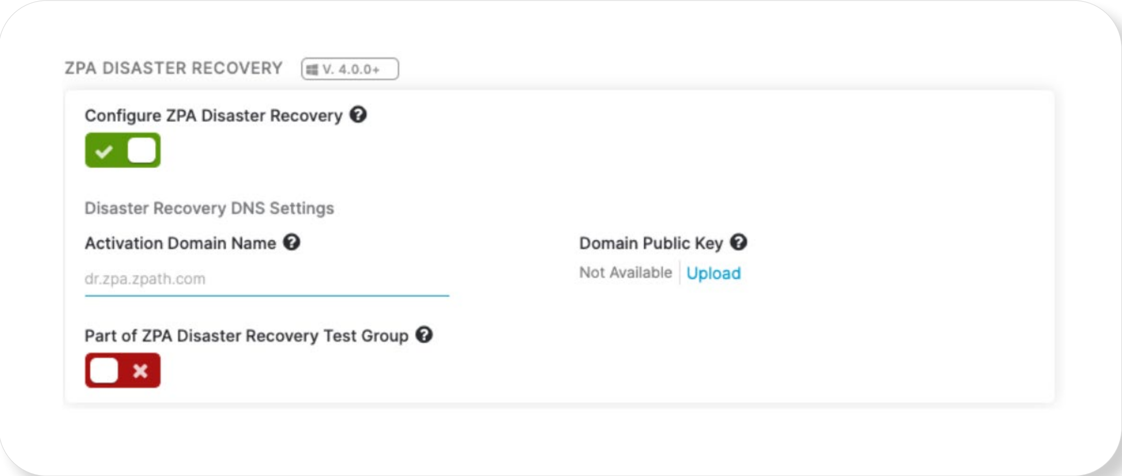
Table 9 ZCC App Profiles Policy ZIA DR Settings

ZPA Configuration

ZPA DR mode allows enrolled and authenticated users to have network-level access to mission critical applications enabled for DR via ZCC, when the ZPA service is not accessible. Unlike ZIA, ZPA DR is configured using both the ZCC and the ZPA Admin Portal.

ZCC Portal Configuration

1. In the ZPA Admin Portal, navigate to the Zscaler Client Connector Portal
2. Click App Profiles
3. For each supported platform (Windows and macOS), edit an existing policy or create a new one as applicable.
4. Scroll to the ZPA Disaster Recovery section and toggle Disaster Recovery service



ZPA DISASTER RECOVERY V. 4.0.0+

Configure ZPA Disaster Recovery ✓

Disaster Recovery DNS Settings

Activation Domain Name: dr.zpa.zpath.com

Domain Public Key: Not Available | Upload

Part of ZPA Disaster Recovery Test Group ✗

5. Configure the ZPA Disaster Recovery settings using the table below.

Settings	Status
Activation Domain Name	Enter the disaster recovery domain name
Domain Public Key	Upload the dr_publickey.pem file created with the Zscaler Record Generator Tool. This key is used to validate the DNS TXT records
Part of ZPA Disaster Recovery Test Group	Zscaler recommends having at least one profile per platform designated as a DR Test Group with a corresponding group of test users.

Table 10 ZCC App Profile ZPA DR Settings

ZPA Portal Configuration

1. Open the portal and navigate the configuration page by clicking to Administration -> Settings ->Disaster recovery -> Settings

2. Configure the ZPA Disaster Recovery Settings using the details in the table below.

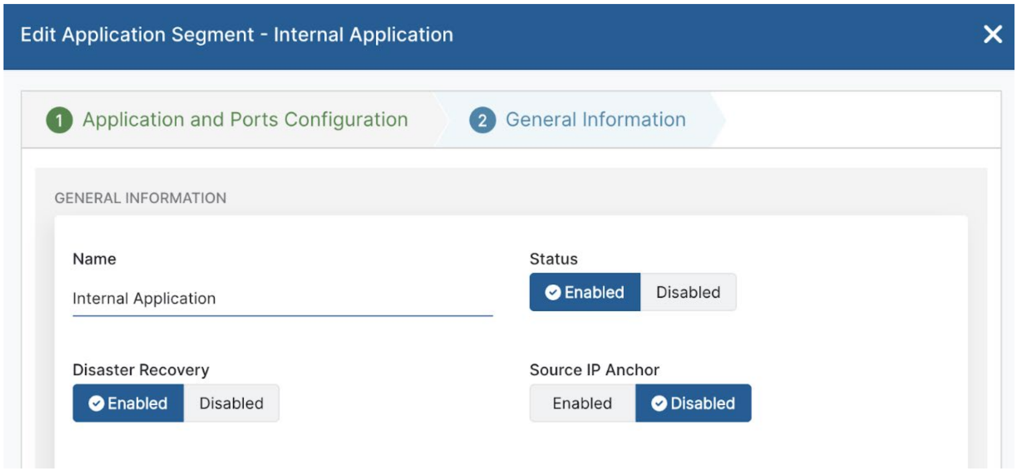
Settings	Status
Max Age for Authentication	This is the set amount of time that the current end-user authentication is valid for during Disaster Recovery Mode. The default maximum age for authentication is 14 days.
Disaster Recovery Public Key	Upload the dr_publickey.pem file created with the Zscaler Record Generator Tool. This key is used to authenticate the DNS TXT records
Disaster Recovery Domain Name	Enter the disaster recovery domain name

Table 11 ZPA Disaster Recovery

3. Go to Administration –> Application Management –> Application Segments

4. Edit the application segment(s) that include the mission-critical applications.

5. Within the Edit Application Segment Screen, click Next to get to General Information


Edit Application Segment - Internal Application
1 Application and Ports Configuration
2 General Information
GENERAL INFORMATION

Name: Internal Application

Status: Enabled (selected) / Disabled

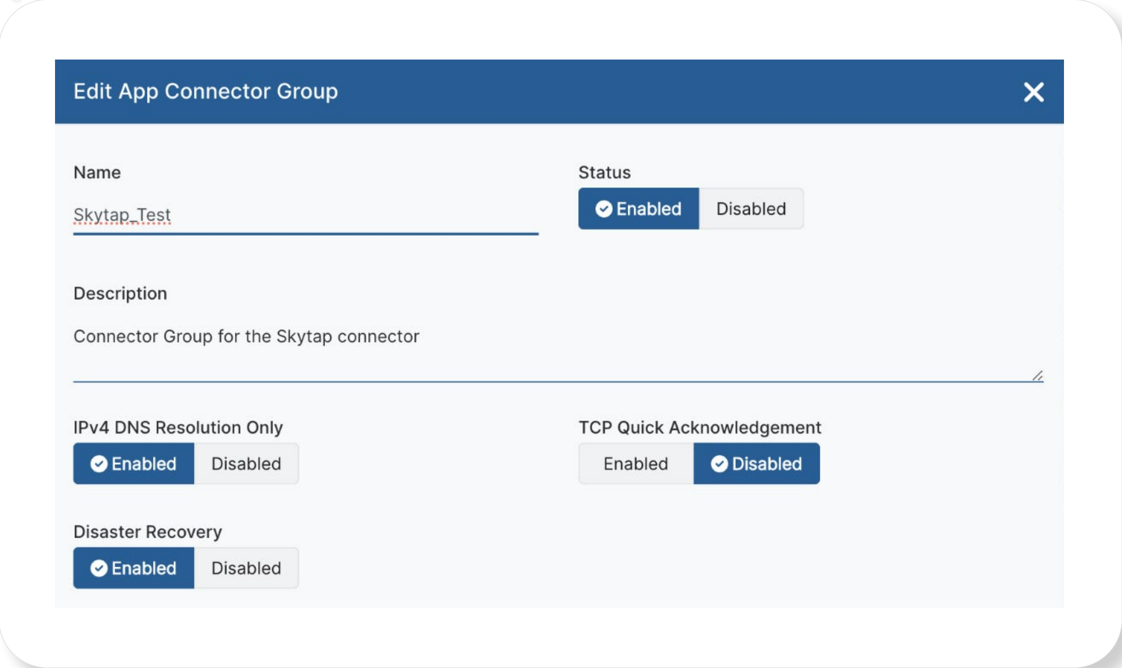
Disaster Recovery: Enabled (selected) / Disabled

Source IP Anchor: Enabled / Disabled (selected)

6. Set Disaster Recovery to Enabled and click Save

7. Go to Administration –> App Connector Management –> App Connector Groups

8. Edit the App Connector Groups that serve the mission critical applications by setting Disaster Recovery to Enabled



Edit App Connector Group

Name: Skytap_Test

Status: [✓ Enabled] Disabled

Description: Connector Group for the Skytap connector

IPv4 DNS Resolution Only: [✓ Enabled] Disabled

TCP Quick Acknowledgement: Enabled [✓ Disabled]

Disaster Recovery: [✓ Enabled] Disabled

9. Click Save.

10. Go to Administration –> Service Edge Management –> Service Edge Groups.

11. Edit the existing Service Edge Groups or create new Service Edge Groups as applicable.

12. Set Disaster Recovery to Enabled.

13. Navigate to Administration–> Service Edge Management –> Service Edges

14. Record the public IP addresses of the PSEs that are members of the DR Enabled Service Edge Groups.

15. Validate there are DNS A records configured in the Disaster Recovery domain resolving to the public IP address of each PSE enabled for DR.

Testing

Zscaler recommends testing Disaster Recovery as part of the initial configuration. Periodic DR testing should be done at least twice a year as part of the organization's existing DR Test Schedule. ZIA DR Traffic Forwarding conditions and may report problems accessing locations blocked or not allowed during DR testing.

For ZIA, only users assigned to App Profiles marked as Part of DR Testing Group will operate using the DR traffic forwarding mode.

ZPA Regular Users under Test Mode

Activating Test Mode will disconnect all users connected to the PSEs and App Connectors enabled for DR Testing. Additional PSEs and App Connectors not enabled for DR test mode must be available to allow regular users to continue accessing applications during the test. Otherwise, any application serviced through the DR PSEs and DR App Connectors will remain inaccessible to non-test users during the test.

ZPA Users in Test Mode

In the case of ZPA, users connecting to Application Segments, App Connectors, and PSEs marked as Part of the DR Test Group will be able to access applications configured for DR. Applications not marked for DR will be inaccessible during the test.

Environments must be sized and segmented appropriately for both regular cloud application access and DR testing to avoid creating a business disruption.

Enable DR Test mode through the following process:

1. Create a DNS TXT record using the Zscaler Record Generator Tool

Generator Tool Prompt	Value	Notes
Signed DNS records?	Yes	Zscaler recommends using signed DNS records when performing DR operations.
Create key pairs?	No	Copy the dr_privatekey.pem file /Program Files/Zscaler Record Generator/Files
Disaster Recovery needs to be configured for ZIA?	Yes	If activating DR test mode for ZIA, otherwise set No
Overwrite ZCC Portal configuration	No	Zscaler recommends using the Pre-defined Destinations option that is only configured in ZCC Portal
Disaster Recovery needs to be configured for ZPA	Yes	If activating DR test mode for ZPA, otherwise set to No
Set the disaster recovery status for the disaster recovery domain;	Test	Only App Profiles, App Segments, App Connectors and PSEs marked as Part of DR Test Groups will enter DR Mode.
Do you want to start disaster recovery now?	No	Enter the activation date in yyyy-mm-dd format and time in UTC using the hh-mm-ss format
Default disaster recovery activation	No	Enter the deactivation date in yyyy-mm-dd format and time in UTC using the hh-mm-ss format

Table 12 Zscaler DNS Record Generator Settings for test mode

2. Upload the DNS TXT records to the DNS server for the disaster recovery domain name to activate Disaster Recovery Test Mode

3. Upon DNS propagation, DR mode will be activated for users and groups configured within App Profiles enabled for both Disaster Recovery and marked as Part of ZIA / ZPA Disaster Recovery Test Group.

4. Test users should validate that access to the Mission Critical Applications (ZPA validation) and internet sites (ZIA) can be achieved. The results of each tested application and site should be documented for audit (pass/fail) and reviewed for changes from previous tests.

5. Instruct test users to try to access non-mission Critical Applications and sites blocked through custom allow lists or not included within Zscaler's predefined Global Allow list and record the results of each test.

6. Failed tests should be remediated by validating existing DR configurations. Modify configurations and conduct additional tests until achieving the expected results.

7. Once testing is complete, create a new DNS TXT Record with a Disaster Recovery Mode (b) tag set to off

NOTE: During DR Test Mode, any PSE and App Connector marked for participation in DR Test Group will reboot, causing all users connected to that PSE and App Connectors to lose connectivity to the applications serviced by those components until they reconnect to non-DR marked App Connectors and PSEs as applicable.

Deactivating Disaster Recovery

DR mode will deactivate once the current time exceeds the end time included in the DNS TXT Record. To deactivate DR before that time, create a new DNS TXT record using the Zscaler Record Generation Time with the following settings.

Generator Tool Prompt	Value	Notes
Signed DNS records?	Yes	Zscaler recommends only using signed records to perform DR operations.
Create key pairs?	No	Copy the dr_privatekey.pem file /Program Files/Zscaler Record Generator/Files
Disaster Recovery needs to be configured for ZIA?	Yes	If deactivating DR test mode for ZIA, otherwise set No
Overwrite ZCC Portal configuration	No	Zscaler recommends using the Pre-defined Destinations option that is only configured in ZCC Portal
Disaster Recovery needs to be configured for ZPA	Off	If deactivating DR test mode for ZPA, otherwise set to No
Set the disaster recovery status for the disaster recovery domain;	Test	Deactivates DR Mode
Do you want to start disaster recovery now?	Yes	Deactivation will take place upon uploading the DNS TXT record
Default disaster recovery activation	Ignore	Value is not required

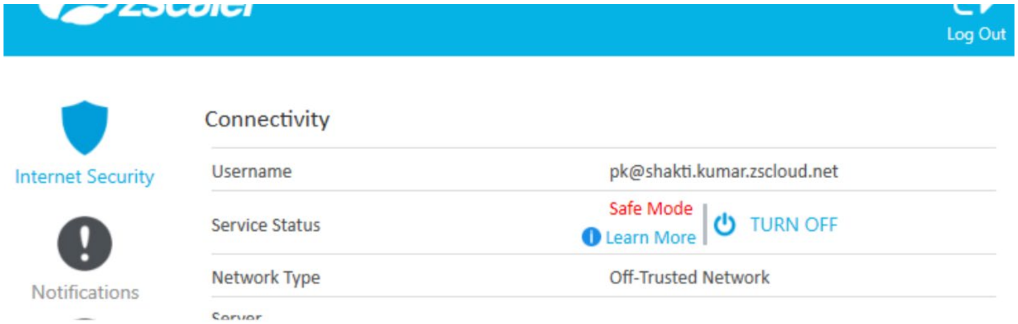
Table 13 DNS settings for Test Mode DNS TXT Records

User Experience during Disaster Recovery

Once DNS TXT records are uploaded ZCC, App Connectors and PSEs will detect activation and enter DR Mode. The user experience is as follows:

ZIA Users

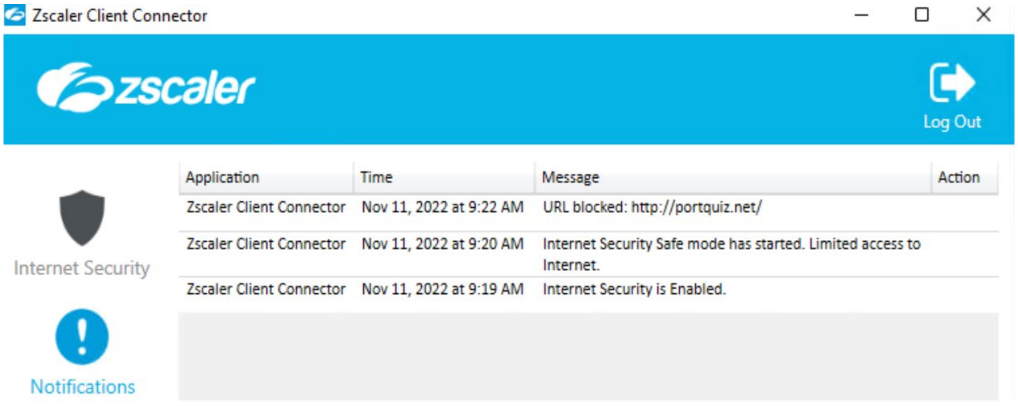
- Users may experience an interruption if browsing the internet
- The Internet Security Section within ZCC will display "Safe Mode" in the Service Status section



Connectivity

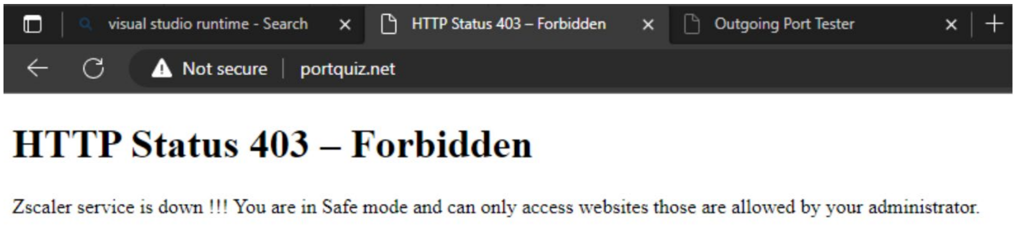
Username	pk@shakti.kumar.zscloud.net
Service Status	Safe Mode Learn More | TURN OFF
Network Type	Off-Trusted Network
Server	

- Log entries will be created within the Notifications Section of ZCC



Application	Time	Message	Action
Zscaler Client Connector	Nov 11, 2022 at 9:22 AM	URL blocked: http://portquiz.net/	
Zscaler Client Connector	Nov 11, 2022 at 9:20 AM	Internet Security Safe mode has started. Limited access to Internet.	
Zscaler Client Connector	Nov 11, 2022 at 9:19 AM	Internet Security is Enabled.	

- Users may see an HTTP 403 error for blocked destinations.



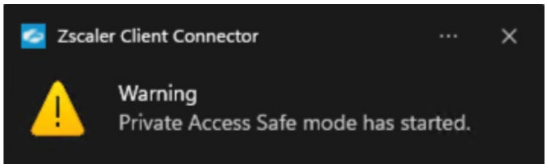
HTTP Status 403 – Forbidden

Zscaler service is down !!! You are in Safe mode and can only access websites those are allowed by your administrator.

ZPA Users

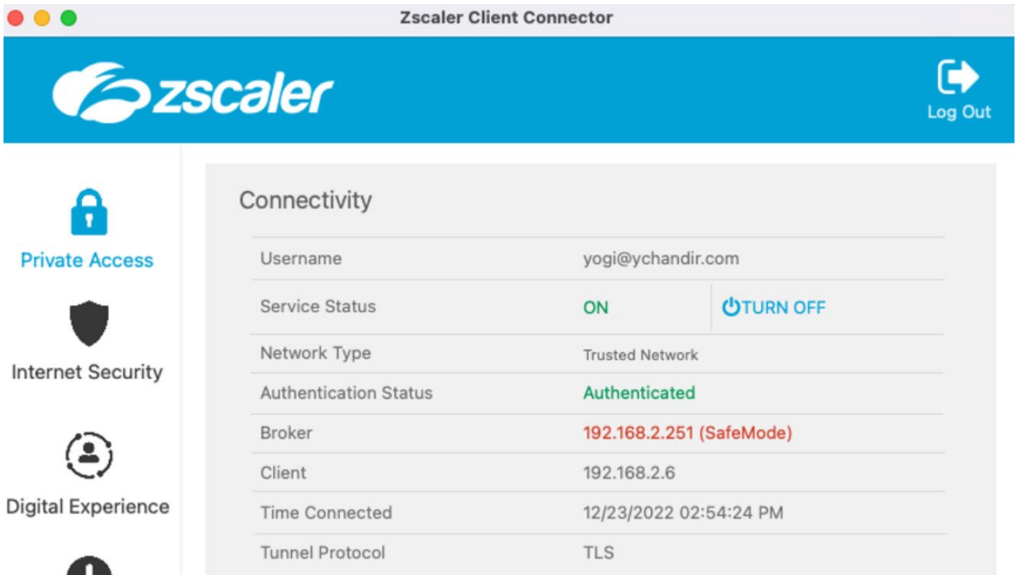
Once App Connectors and PSEs detect DR mode activated, they will reboot, dropping all connections. Users may be disconnected for 30 seconds until ZCC connects to a DR-enabled PSE. From that point, forward users will have network-level access to mission critical applications enabled for DR. The user experience is as follows:

- Once ZCC detects DR mode the user will receive a Safe Mode popup notification.



Warning
Private Access Safe mode has started.

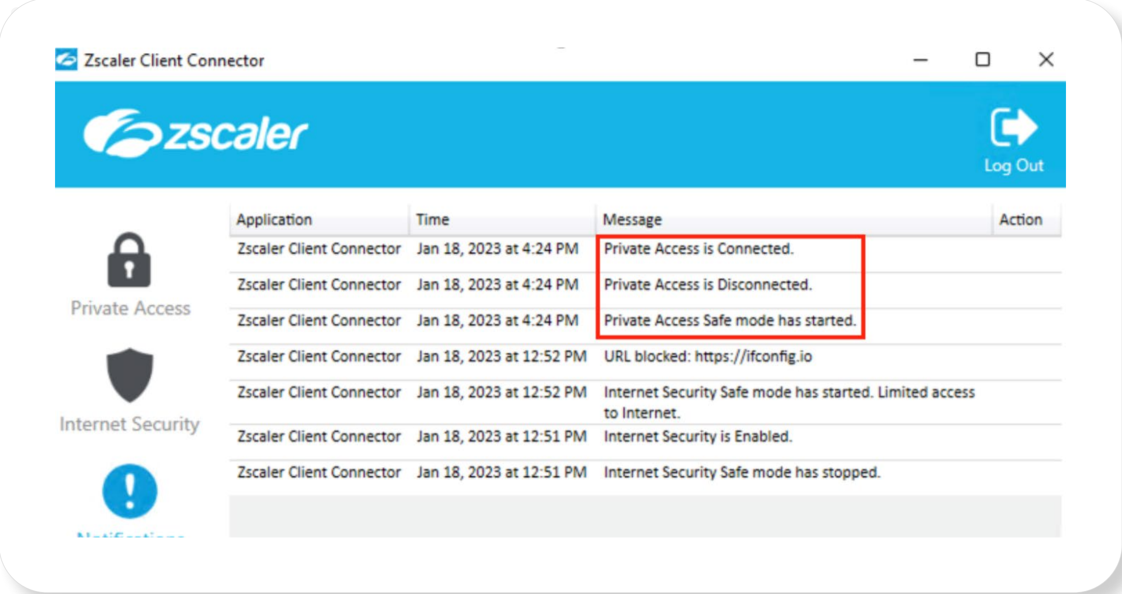
- The Private Access section within ZCC will display "Safe Mode" in the Broker section



Connectivity

Username	yogi@ychandir.com	
Service Status	ON	TURN OFF
Network Type	Trusted Network	
Authentication Status	Authenticated	
Broker	192.168.2.251 (SafeMode)	
Client	192.168.2.6	
Time Connected	12/23/2022 02:54:24 PM	
Tunnel Protocol	TLS	

- Log entries will be created within the Notifications Section of ZCC



Application	Time	Message	Action
Zscaler Client Connector	Jan 18, 2023 at 4:24 PM	Private Access is Connected.	
Zscaler Client Connector	Jan 18, 2023 at 4:24 PM	Private Access is Disconnected.	
Zscaler Client Connector	Jan 18, 2023 at 4:24 PM	Private Access Safe mode has started.	
Zscaler Client Connector	Jan 18, 2023 at 12:52 PM	URL blocked: https://ifconfig.io	
Zscaler Client Connector	Jan 18, 2023 at 12:52 PM	Internet Security Safe mode has started. Limited access to Internet.	
Zscaler Client Connector	Jan 18, 2023 at 12:51 PM	Internet Security is Enabled.	
Zscaler Client Connector	Jan 18, 2023 at 12:51 PM	Internet Security Safe mode has stopped.	

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.