

# verizon Zero Trust Dynamic Access Service Description User Manual

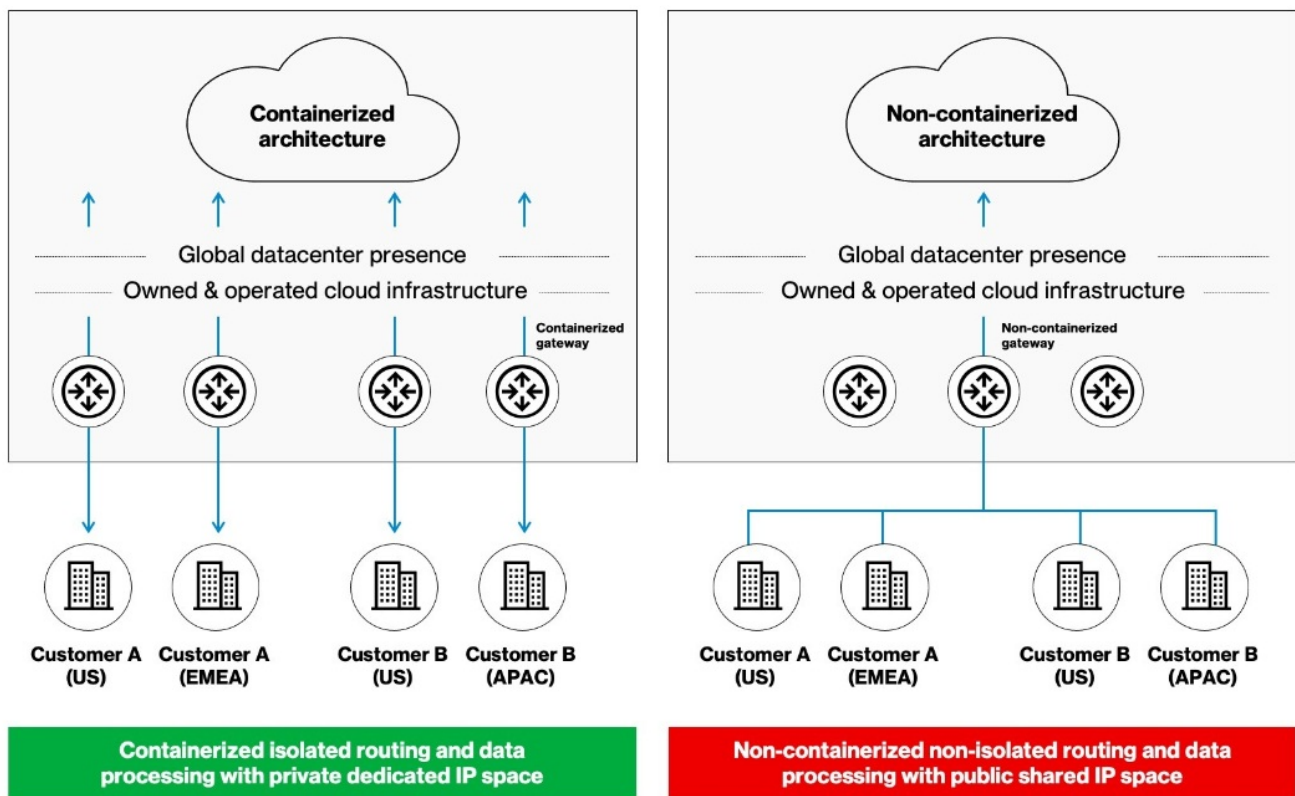
[Home](#) » [Verizon](#) » verizon Zero Trust Dynamic Access Service Description User Manual 

## Contents

- 1 [verizon Zero Trust Dynamic Access Service Description](#)
- 2 [Product Information](#)
- 3 [Product Usage Instructions](#)
- 4 [Zero Trust Dynamic Access Service Description](#)
- 5 [Overview](#)
- 6 [Zero Trust Dynamic Access Packages & Features](#)
- 7 [Deployment of Zero Trust Dynamic Access](#)
- 8 [Customer Support](#)
- 9 [Documents / Resources](#)
  - 9.1 [References](#)
- 10 [Related Posts](#)



**verizon Zero Trust Dynamic Access Service Description**



## Product Information

### Specifications

- Product Name: Zero Trust Dynamic Access
- Package Levels: Core, Advanced, Complete
- Features: Essential security controls, advanced threat protection, VPN replacement, data loss prevention (DLP), API CASB capabilities

### Overview

The Zero Trust Dynamic Access is a cloud security offering that provides essential security controls for both on- and off-network users and devices. It offers different package levels with increasing features to meet various security needs.

## Zero Trust Dynamic Access Packages & Features

### Core Package Features

The Core Package is the base-level offering and includes the following standard Zero Trust service edge features:

- Essential security controls for on- and off-network users and devices

### Advanced Package Features

The Advanced Package includes all the Core Package features, plus:

- Advanced threat protection
- Ability to connect users to private on-premises resources for VPN replacement
- Signature-based intrusion detection and prevention
- Real-time intrusion, malware, and virus protection

- Event detail viewing with source and destination IP addresses
- Automatic signature threat feed subscriptions
- Category-based malware rules
- Visual rule creation and editing
- Integration with Microsoft Azure AD, Microsoft Defender for Cloud Apps, Microsoft Sentinel, Microsoft Purview Information Protection (MIP), Microsoft 365

### **Complete Package Features**

The Complete Package is the most comprehensive offering and includes all the Core and Advanced Package features, plus

- Data loss prevention (DLP)
- API CASB capabilities
- Comprehensive file-based data loss prevention capabilities
- Automated alerts for unauthorized data transfer
- Out-of-band API CASB for fine-grained controls and visibility into cloud applications
- Inline data loss prevention (DLP) for scanning all traffic for Personally Identifiable Information (PII) data
- Advanced detection capabilities to prevent unintended loss of sensitive information
- Advanced content analysis engines for processing and parsing targeted files

## **Product Usage Instructions**

### **Core Package Usage**

To utilize the Core Package features

1. Ensure that the Zero Trust Dynamic Access service is properly set up and configured.
2. For on-network users and devices, the essential security controls will automatically be applied.
3. For off-network users and devices, follow the provided instructions to establish a secure connection to the Zero Trust service edge.

### **Advanced Package Usage**

To take advantage of the Advanced Package features:

1. Ensure that the Core Package is activated and functioning correctly.
2. Enable advanced threat protection by configuring the intrusion detection and prevention settings.
3. To connect users to private on-premises resources, follow the provided instructions for VPN replacement setup.
4. Integrate with Microsoft Azure AD, Microsoft Defender for Cloud Apps, Microsoft Sentinel, Microsoft Purview Information Protection (MIP), and Microsoft 365 for enhanced security capabilities.

### **Complete Package Usage**

To utilize the Complete Package features:

1. Ensure that both the Core and Advanced Packages are activated and functioning correctly.
2. Enable data loss prevention (DLP) by configuring the necessary settings to detect and prevent the transfer of

sensitive data to unauthorized locations in the cloud.

3. Utilize the API CASB capabilities to apply fine-grained controls and gain visibility into cloud applications.
4. Take advantage of advanced detection capabilities and content analysis engines to prevent unintended loss of sensitive information.

## FAQ

- **Q: What is the Zero Trust Dynamic Access service?**

A: The Zero Trust Dynamic Access service is a cloud security offering that provides essential security controls for both on- and off-network users and devices.

- **Q: What are the package levels available?**

A: There are three package levels available: Core, Advanced, and Complete.

- **Q: What features are included in the Core Package?**

A: The Core Package includes essential security controls for on- and off-network users and devices.

- **Q: What features are included in the Advanced Package?**

A: The Advanced Package includes all the Core Package features, plus advanced threat protection and the ability to connect users to private on-premises resources for VPN replacement.

- **Q: What features are included in the Complete Package?**

A: The Complete Package includes all the Core and Advanced Package features, plus data loss prevention (DLP) and API CASB capabilities.

## Zero Trust Dynamic Access Service Description

© 2022 Verizon. All rights reserved. Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Verizon and are protected by patent, copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited without the prior written permission of Verizon.

## Acronym Definitions

- CASB – Cloud Access Security Broker
- CCN – CMS Certification Number
- DLP – Data Loss Prevention
- DNS – Domain Name System
- IAM – Identity and Access Management
- ICAP – Internet Content Adaptation Protocol
- IdP – Identity Provider
- IoT – Internet of Things
- MFA – Multi Factor Authentication
- NIST – National Institute of Standards and Technology
- OT – Operational Technology
- PEP – Policy Enforcement Point
- PII – Personally Identifiable Information
- SaaS – Security as a Service
- SCP – Secure Copy Protocol

- SFTP – Secure File Transfer Protocol
- VDI – Virtual desktop infrastructure
- VPN – Virtual private network
- WCCP – Web Cache Communications Protocol. (Cisco-developed content-routing protocol) ZTA – Zero Trust Access

## Overview

- Verizon's Zero Trust Dynamic Access helps to prevent breaches by making applications, data and services virtually inaccessible to attackers while allowing trusted users to securely and directly connect to protected resources. Zero Trust Dynamic Access provides a zero trust cloud security solution for secure access to the open internet, cloud applications, private applications and data, and public cloud services helping to ensure security and compliance and providing reporting. Zero Trust Dynamic Access cloud security platform is provided by iboss, a leading cybersecurity company.
- Companies are moving to a 'Zero Trust' model of cyber security which takes the approach that no users or devices are to be trusted without continuous verification, while limiting potential system response latency. The main drivers for a Zero Trust architecture include the frequency of target-based ransomware and cyber-attacks, increasing regulations for data protection and information security and the fact that users and resources are now distributed outside of the office making them accessible by attackers.
- Trust Dynamic Access is specifically designed to meet the cybersecurity needs of today's distributed organizations. Built for the cloud as a SaaS offering, Zero Trust Dynamic Access can defend today's complex and decentralized networks, branch offices, and the remote and mobile users that depend on them. Zero Trust Dynamic Access provides the flexibility required to drop-in and replace existing on-premises legacy secure web gateway (SWG), virtual private network (VPN), and virtual desktop infrastructure (VDI) solutions, helping organizations to transition to a Zero Trust architecture smoothly, without the need to re-architect their existing networks.
- A distinct advantage of Zero Trust Dynamic Access is based on its containerized architecture which allows security to not only be placed close to the user, but also allows security to be close to the resource regardless of where the resource resides. It does this by stretching the secure service edge near data and applications, such as those within a datacenter, while maintaining a single, unified service edge which helps guarantee consistent security, policies and visibility across all users and resources. This design also can enable the most direct to resource connections without forcing data through unnecessary paths which helps ensure the fastest and lowest latency connections.

## Zero Trust Dynamic Access Packages & Features

Zero Trust Dynamic Access is available in three packages – Core, Advanced, and Complete. All packages come with 500 GB of Cloud Storage for logging, reporting and analytics at no additional cost.

### Core Package Features

The Core Package is the base-level cloud security offering that provides essential security controls for both on- and off-network users and devices and includes the following standard Zero

### Trust service edge features

- Security controls – Cloud security controls including blocking malicious sources, web filtering and compliance policies
  - Content-based analysis and inspection
  - Dynamic policies based on user and group membership
  - Stream-based protection, including all ports and protocols (TCP & UDP)
  - Granular category- and user-based filtering
  - Alerts based on keywords, events, and other customizable triggers
  - File extension, domain extension, and content MIME type blocking
  - Port access management
  - Dynamically updated URL database
  - DNS Security for guest networks, BYOD, Internet of Things (IoT), and Operational Technology (OT) device protection
  - Policies for blocking access to harmful online content and to help ensure an organization is compliant with data privacy and protection policies and regulations
- SaaS and social media controls – Provide granular in-app controls to enforce compliance and reduce risk
  - Advanced application scanning and deep content inspection
  - Content-aware management of social media applications like Facebook, Twitter, LinkedIn, and Pinterest
  - SafeSearch enforcement for Google, Bing, and Yahoo
  - Clean image search and translation filtering for Google services
- Advanced proxy rules & actions – Block, allow, redirect, manipulate http headers, force or bypass authentication requirements, forward to external ICAP.
- Protection for out-of-date browsers and operating systems – helps to extend the protection of deployed technologies after end-of-life (EOL), when vendors stop issuing security updates and patches.
- User and group-based access policies via cloud connectors – Support for Windows, Mac, iOS, Chromebook, Linux, and Android devices for extending cybersecurity coverage to managed devices with connectivity regardless of where they are located.
- Encrypted traffic inspection and protection (HTTPS Decrypt) – Apply security policies against encrypted (HTTPS/SSL) traffic. Micro-segmentation to selectively decrypt based on content, device, user, or group.
- Resource catalog (apps, data, services), user catalog, asset catalog – a catalog of over 5000+ 3rd party public cloud resources that are classified by type and risk level which an organization may choose to connect to the Policy Enforcement Point, as defined in Section 4.
- Resource tagging – Ability to tag resources by type, location, and risk classification.
- Zero Trust NIST 800-207 criteria-based access policies – Enables privilege-based access to resources through definition of criteria necessary for a user to access a resource. (e.g., by geo-location, specific user, user group membership from federated identity providers (like Okta, Ping, Microsoft AD, etc.).
- Connect cloud accessible resources – Connect to and protect any proprietary applications with a publicly accessible IP address.
- Dedicated static IP – Allows anchoring resources to the Policy Enforcement Point, making resources inaccessible through the public internet (e.g., restrict access to Salesforce).
- Policy tracing – Ability to troubleshoot policies (e.g., if a specific policy is used to block access to a resource).
- Reporting & analytics – Overview dashboard including reporting, analytics, logs, report templates, etc.
- Zero Trust dashboard – Reporting by resource type, resource location, and security impact level.

## Advanced Package Features

The Advanced Package is the mid-level offering that includes all the Core Package features, plus advanced threat protection and the ability to connect users to private on-premises resources for VPN replacement.

- Advanced malware detection and prevention – Malware identification and mitigation from top-ranked signature and signature-less engines, iboss proprietary malware registry, and integration with the Verizon Threat Research Advisory Center (VTRAC) feed.

<https://www.iboss.com/best-of-breed-malware-defense-2/>

- Behavioral malware sandboxing – Auto or manual deposit of user downloaded files for behavioral sandboxing analysis.
  - Blended AV scanning
  - Malware rules for more granular control over malware content analysis
- Signature-based intrusion detection and prevention:
  - Real-time intrusion, malware, and virus protection
  - Quickly and easily view event detail, including source and destination IP addresses
  - Automatic signature threat feed subscriptions
  - Category-based malware rules
  - Visual rule creation and editing
- Phishing prevention – Dozens of leading threat and phishing feeds automatically included in the platform – e.g., PhishTank, SpamHaus, VTRAC.
- Infected device detection and isolation (Command and Control Callback Prevention) –Domain, URL, and blacklisted IP monitoring. Geolocation identifies the origination point of callbacks.
- Integration with 3rd party federated identity providers – Eliminate unauthorized users by integrating with federated identity providers (e.g., Okta, Ping, Microsoft AD, etc.).
- Extend modern authentication (SAML/OIDC) to legacy apps & resources – Ensures modern authentication including MFA can be enforced on all resources, including legacy applications that have no ability to integrate with federated identity services.
- Concurrent in-line CASB – The ability to apply fine grained controls and gain visibility into cloud application use. This includes making Facebook read-only, ensuring access to Google
- Drive is corporate only and leveraging Microsoft365 Tenant restrictions.
- Connect resources on private networks – Supports connections via tunnels, SD WAN, WCCP) to Policy Enforcement Points.
- Continuous Adaptive Access Controls –
  - Automatically cut access to resources when a device is infected with malware
  - Adaptively change resource access policies based on device posture checks including ensuring the firewall is enabled and disk is encrypted
  - Zero trust scoring algorithms – adaptively use signals to grant or deny access to protected resources such as ensuring access is only allowed from specific regions or only from enterprise-owned devices
  - Continuous per-request access decisions extend conditional access decisions beyond the point of login and apply to every request between a user and a resource
- Threat dashboard – Displays blocked malware, phishing, malicious sources.
- Zero trust dashboard – Resource score-based reporting and continuous scoring of each logged transaction provides insights into changes in risk. Resources may consist of applications, systems, etc.
- Zero trust incidents dashboard – provides access to subject and asset incident information including infected

devices and users with active incidents.

- Log forwarding – stream logs to local SIEM or database via Syslog, Secure Copy Protocol (SCP), Secure File Transfer Protocol (SFTP) directly from the cloud which contain events including web access logs, malware events and data loss alerts.

<https://www.iboss.com/business/stream-cloud-logs-to-external-siem/>

- Microsoft integration – <https://www.iboss.com/storage/2022/05/2022-05-iboss-microsoft-integration.pdf>
  - Microsoft Azure AD
  - Microsoft Defender for Cloud Apps
  - Microsoft Sentinel
  - Microsoft Purview Information Protection (MIP)
  - Microsoft 365

### **Complete Package Features**

The Complete Package is the most comprehensive offering. It includes all the Core and Advanced Package features, plus data loss prevention (DLP) and API CASB capabilities.

The Complete Package offers comprehensive file-based data loss prevention capabilities that help to detect and stop the transfer of sensitive data to and from unauthorized locations in the cloud while keeping security teams informed with automated alerts. This helps to provide protection against unauthorized cloud use and sensitive data loss protection for the use of the cloud, that can ensure that sensitive data is secured and maintained within organizationally approved cloud services.

- **Out-of-band API CASB** – The ability to apply fine grained controls and gain visibility into cloud applications. Inspects data at rest. <https://www.iboss.com/platform/casb/>

Inline data loss prevention (DLP) (PII, CCN) – Scans all traffic, looking for Personally Identifiable Information (PII) data in any transaction going through the iboss service. <https://www.iboss.com/platform/dlp/>

### **Advanced Detection Capabilities**

- Screen content to help prevent unintended loss of sensitive information.
- Capable of scanning: Credit card numbers, PII, email addresses, phone numbers.
- Support regular expressions (regex) to search for text strings deep within transferred content.

### **Advanced Content Analysis Engines**

- Process and parse targeted files, that can ensure that even compressed content is accessible to the detection engines.
- Set compressed file max scan depth to search for content deep within zip files.
- Analyzes numerous file types including: Base16, GZip, PDF, Outlook data files, SQLite Database, Windows PE Executables, Zip files, RAR files, Windows Hibernate Files, Windows LNK files, Windows PE Files.

### **Optional Package Add-Ons**

- Cloud storage options – 500GB of log storage on the iboss cloud is included at no additional cost. Logs can be streamed to external log storage/SIEM solutions or deleted based on parameters controlled via the admin portal. Additional cloud storage can be purchased if required.



- Regional surcharges – Additional surcharges will apply when cloud gateways need to be located in multiple locations (Zone 1 – US, Canada, Mexico, UK, Belgium, Bulgaria, Denmark, Finland, France, Germany, Helsinki, Ireland, Italy, Netherlands, Norway, Poland, Spain, Sweden, Switzerland, Turkey, Mexico City, Singapore). Additional surcharges will also apply when Cloud Gateways need to be located in certain countries to account for higher data center prices (Zone 2 – Columbia, Israel, S. Africa, India, South Korea, Japan, Hong Kong, Australia, Brazil and Zone 3 – China, UAE, Egypt, Taiwan, New Zealand, Argentina).
- Remote browser isolation – Browser isolation limits sensitive data leaks from unmanaged device use and helps protect users from threats when accessing high-risk web sites. Ideal for Virtual Desktop Infrastructure (VDI) replacement.  
<https://www.iboss.com/platform/browser-isolation/>
- Private cloud hardware – iboss Policy Enforcement Points (PEPs) can be placed in private data centers (e.g., for regulatory compliance, to be closer to critical resources, to replace existing on-premises hardware proxies, etc.).
- Implementation and Professional Services – Depending upon the project scope and configuration requirements, implementation or professional services fees may apply. The number of Implementation service hours will be determined during pre-sales and included on the customer quote. See Section 5 for a description of included and excluded implementation services.
- Mission Critical Support – See Section 6 for a description of support options.

## Deployment of Zero Trust Dynamic Access

Zero Trust Dynamic Access will be provisioned by iboss, Verizon's third party vendor. After the customer account is provisioned, a welcome letter will be emailed to the designated customer administrator and if needed, an iboss implementation engineer will provide dedicated technical product expertise to assist the customer with onboarding on the cloud platform:

## Implementation Services Provided

- Implementation kickoff call
- Coordination of project & implementation plan with identified milestone and completion dates
- Provide template user acceptance testing spreadsheets and user documents
- Live technical assistance configuring the platform for the following:
  - Assistance creating administrative users in the platform
  - Assistance enabling multi-factor authentication for admin users
  - Review of traffic redirection options
  - Time zone configuration
  - Platform maintenance scheduling
  - Email setting configuration
  - Backup configuration
  - Guidance developing web security groups
  - Assistance integrating with a cloud Identity Provider/Identity and Access Management (IdP/IAM)
  - Assistance creating a customized SSL decryption certificate
  - Assistance downloading and configuring iboss cloud connectors for required device types (up to 5 devices)
  - Guidance on resource categorization

- Guidance on configuring trust algorithms
- Guidance on policy configuration
- Creation of 1 custom branded block page
- Creation of 1 custom report schedule
- Creation of 1 custom IPS rule
- Customization of 1 PAC script
- Integration with 1 external SIEM for logging

### **Implementation Services Excluded**

- Mass deployment, updates, or removal of cloud connectors in a customer's environment
- Active Directory, Azure, eDirectory or other directory service configuration or support
- Mobile Device Management (MDM) configuration or support
- Policy migration from legacy on-prem gateway proxies or firewall
- Configuration of customer firewalls, routers, switches, computers, or third-party software or applications

### **Private Cloud Deployment Option**

- Zero Trust Dynamic Access is delivered as a complete SaaS offering in the cloud without the need for on-premises appliances. In some cases, however, a customer may want to extend the service into a "private cloud" deployment. The containerized architecture of the solution allows the cloud configuration to extend into an optional private cloud Point of Presence (PoP). The private cloud is a dedicated on-premises gateway capacity that can be used to replace existing legacy proxies. The private cloud POP is shipped directly to the customer premises for installation.
- Because the private cloud is just an extension of the global cloud, any policies or controls configured within the platform can automatically extend into the private cloud PoP. The private cloud becomes part of the global cloud extending it to private points of presence. This provides the consistency in security and user experience necessary when extending into a private cloud since a single policy-set and a single pane of glass is used for administration.

<https://www.iboss.com/platform/extend-iboss-cloud-into-private-cloud/>

### **Customer Support**


Zero Trust Dynamic Access is offered with two customer support packages: Standard Support and Mission Critical Support delivered by iboss, Verizon's third party vendor, as described below.

| <b>iboss Support Packages</b>        | <b>Standard</b>                                      | <b>Mission Critical</b> |
|--------------------------------------|--|-------------------------|
| Online Support Center Access         | included   | included                |
| Knowledge Base                       | included   | included                |
| Online Training, Videos, User Guides | included   | included                |
| iboss Named Support Contacts         | 0  | 2                       |
| Live Support Hours                   | 8am-8pm EST Monday-Friday (excluding major holidays) | 24/7                    |
| Professional Services                | Not Included   | Up to 1 hr/month        |
| Severity Level 1 Response Time       | 2 hours  | 15 minutes              |

|                                |   |   |
|--------------------------------|---|---|
| Severity Level 2 Response Time | 4 hours   | 1 hour  |
| Severity Level 3 Response Time | 24 hours  | 4 hours   |
| <b>Pricing</b>                 | <b>Included in All Packages at no additional charge</b> | <b>Additional charge based on number of users</b> |

© 2022 Verizon. All rights reserved. Proprietary & Confidential Statement: This document and the information disclosed within, including the document structure and contents, are confidential and the proprietary property of Verizon and are protected by patent, copyright and other proprietary rights. Any disclosure to a third party in whole or in part in any manner is expressly prohibited without the prior written permission of Verizon.

## Documents / Resources

|   |  |
|---|--|
|  | <a href="#">verizon Zero Trust Dynamic Access Service Description</a> [pdf] User Manual<br>Zero Trust Dynamic Access Service Description, Trust Dynamic Access Service Description, Dynamic Access Service Description, Access Service Description, Service Description, Description |
|---|--|

## References

- [🔒 Best Malware Defense - iboss](#)
- [🔒 Stream Cloud Logs to External SIEM - iboss](#)
- [🔒 Provide Contractors, 3rd Parties & BYOD Secure Access to Resources with Browser Isolation - iboss](#)
- [🔒 CASB Provides In-App Controls for Granular Access Decisions - iboss](#)
- [🔒 Extend iboss cloud into Private Cloud - iboss](#)
- [User Manual](#)

