

# Entity Attribute Screens

This section provides the list of **Entity** attribute screens in RiskVision.

The screenshot shows the 'Addresses' tab for a vendor entity named 'Vendor: 361 Degrees'. The left sidebar contains a menu with options: General, Summary, Assessments, Owners, Addresses (selected), Vendor Contacts, Engagements, Documents, and Engagemnt Summary. The main content area is titled 'Address' and shows a table with 2 rows of address data. Above the table are buttons for 'New', 'Edit', 'Delete', and 'More Actions...'. A filter dropdown is set to 'Show all' and a 'Refresh' button is present.

<input type="checkbox"/>	Location	Type	Address	City	State	Postal Code	Country
<input type="checkbox"/>	Mailing	Primary Address	260 Beach	Shanghai	CN	94107	China
<input type="checkbox"/>	Billing	Billing Address	260 Beach	Shanghai	CN	94107	China

*The Addresses tab of a vendor.*

The screenshot shows the 'Description' tab for an application entity named 'Application: Application One'. The left sidebar contains a menu with options: General, Assessments, Owners, Description (selected), Addresses, Classification, Costs & Impact, Vulnerabilities, Vulnerabilities List, Relationships, Propagation, Documents, Data Feeds, and Exceptions. The main content area is titled 'Description' and contains sections for 'Description', 'Network Access', and 'Profile Information'. The 'Description' section lists 'Publisher N/A', 'Version N/A', and 'Accounts N/A'. The 'Network Access' section lists 'IP address N/A', 'Port(s) N/A', and 'Internet facing N/A'. The 'Profile Information' section shows 'Entity Profile(s) High Baseline'.

Description	
Publisher	N/A
Version	N/A
Accounts	N/A
Network Access	
IP address	N/A
Port(s)	N/A
Internet facing	N/A
Profile Information	
Entity Profile(s)	High Baseline

*The Description tab of an application type entity.*

Network Interface: 172.31.4.5 Edit

General

### Network Interface

---

**Network**  
 Unique name 172.31.4.5  
 Domain name N/A  
 Host name 172.31.4.5

**Network Interface**

**⚠** If this interface was discovered automatically, it may also be updated or removed automatically. Because of this, changes made here can be lost without warning.

Description N/A  
 Friendly name nif 172.31.4.5/32  
 MAC address 00:03:B2:2A:C3:46  
 IP address 172.31.4.5  
 Subnet mask 255.255.255.0  
 Network address 172.31.4.0  
 Network zone N/A  
 Wireless No  
 Gateway N/A  
 DNS servers N/A  
 DHCP Enabled No  
 DHCP server N/A  
 DHCP lease obtained N/A  
 DHCP lease expires N/A  
 WINS Server No  
 Primary WINS server N/A  
 Secondary WINS server N/A

*The General tab of a network interface.*

Application: Application One Edit Favorites

General
Assessments
Owners
Description
Addresses
Classification
Costs & Impact
Vulnerabilities
Vulnerabilities List
Relationships
Propagation
Documents
Data Feeds
Exceptions

### Business Criticality

---

Business Criticality  High

### Security Requirements

[Refresh](#)

Confidentiality  High  
 Integrity  Medium  
 Availability  Medium  
 Accountability  Medium

### Classification

---

Classification Label N/A  
 Type Of Data N/A  
 Environment Type N/A  
 Internal or external N/A

▶ [Tags](#)

---

▶ [Change History](#)

*The Classification tab of an application type entity.*

Clicking the **Refresh** button will:

- Update the criticality based on the classification survey; and
- Update any changes made to the classification through the entity user interface.

## General

CVSS v2.0 Score

Identification

More Information

References

Risk

Entities

Custom tab 1

Custom tab 2

Enhanced Score

Risk Score

CVSS v3.0 Score

## ▼ Vulnerability Instance

Entity	10.10.16.101	External reference	N/A
Location	10.10.16.101	Total exposure	N/A
Reported by	eEyeRetina	Secondary source	N/A
First detected	2015-09-17	Issue Id	N/A
Last detected	2015-09-17	Test url	N/A
Fixed	No	File name	N/A
Fixed date	N/A	Line number	N/A
Severity for this entity	High	Discovery method	N/A
Risk for this entity	High	Virtual	No
Resolution status	Unresolved	Exception Status	N/A
Comments	N/A	Exception Current Stage	N/A
Include in report	Yes		
Author	N/A		
CVSS Base Score	10.0		

## ▼ Vulnerability

Title	CVE-1999-0535
Description	A Windows NT account policy for passwords has inappropriate, security-critical settings, e.g. for password length, password age, or uniqueness.
Identifier	CVE-1999-0535
References	N/A
Severity	High
Likelihood	N/A
Weaknesses	N/A
Source	National Vulnerability Database
Status	N/A
System Info	New from Feed
Applicable	Yes

**i** You can decide to always ignore this vulnerability for all entities by marking it not applicable.

*The Description of an Entity Vulnerability.*