D-Link®
Building Networks for People

Network Security Firewall Identidy Awareness Agent User Guide

NetDefendOS

Ver. 1.07.01

Network Security Solution http://www.dlink.com

NetDefend

IDA Administration Guide

DFL-260E/860E/870/1660/2560/2560G

IDA Version 1.07.01

D-Link Corporation
No. 289, Sinhu 3rd Rd, Neihu District, Taipei City 114, Taiwan R.O.C.
http://www.DLink.com

IDA Administration Guide
DFL-260E/860E/870/1660/2560/2560G

IDA Version 1.07.01

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. D-Link makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. D-Link reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

List of Figures

Preface

Intended Audience

This publication is designed to provide a NetDefendOS administrator with details of how to install and administer the *Identity Awareness Agent* (IDA) software. This guide should be used in conjunction with the *Identity Awareness* section of the separate *Administration Guide*.

Trademarks

Certain names in this publication are the trademarks of their respective owners.

NetDefendOS is a trademark of D-Link. Windows and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Highlighted Content

Sections of text which the reader should pay special attention to are indicated by icons on the left hand side of the page followed by a short paragraph in italicized text. Such sections are of the following types with the following purposes:

Note

This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasized, or something that is not obvious or explicitly stated in the preceding text.

Tip

This indicates a piece of non-critical information that is useful to know in certain situations but is not essential reading.

Caution

This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important

This is an essential point that the reader should read and understand.

Warning

This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Chapter 1: IDA Overview

Introduction

This guide describes the installation and administration of the *Identity Awareness Agent* (IDA) software. The IDA software is a component of the NetDefendOS *identity awareness* feature which is used for authentication of remote clients. This guide can be seen as an extension of the identity awareness description which can be found in the authentication section of the *Administration Guide*.

The Software is Separate to NetDefendOS

The IDA software is not supplied with NetDefendOS as it is a piece of self-contained software. Instead, it must be downloaded separately from the D-Link website. The IDA software version numbering is also different from NetDefendOS version numbering and new IDA versions may be released at any time.

The Software Runs On Windows Domain Servers

The IDA software runs on one or more Windows domain servers in an active directory, sending back authenticated client information to NetDefendOS so that further authentication is not necessary. The IDA can run on either a domain controller or domain member. Installation of the IDA software on multiple servers will provide redundancy.

Compatible Windows Server Versions

The IDA software can be installed only on Windows Server™ 2008 R2, 2012 or 2016.

Detailed guidelines for installation are described in the next chapter.

Chapter 2: IDA Installation

The latest IDA software release can be downloaded from the D-Link website. The installation file is a self-extracting Windows executable. When the IDA software is installed, it runs as a Windows service called *IDA.exe*.

IDA Installation Requirements

The following should be noted when installing the IDA:

- When installing the IDA software, the user **must** have administrator privileges.

- When the IDA software is installed on a server that is not an Active Directory Domain Controller, it must be started using an account that has the privileges to allow the reading of the Security Event Log of the Domain Controller.

- It is recommended to run the IDA software at a lower priority than other processes.

- The IDA software must have permissions to do the following:

  i. Read from the event log. To do this a user must be a member of the *Event Log Readers* user group. This group can be found in the *Builtin* Active Directory container.

  ii. Query the Active Directory for users and groups.

  Note: Underscore replaces spaces in NetDefendOS group names

  A group name on the domain controller server can contain spaces but when it is specified in NetDefendOS, spaces in the name must be replaced by the underscore character "_".

- The IDA software can also run as the Local System account.

  If the Remote Event Log Monitoring feature is required, an account for the computer where IDA is installed should be added to the *Event Log Readers* user group.

Note: Troubleshooting installation issues

*If there are issues which occur during installation of the IDA and the problem is not immediately clear, it can be useful to open the **Windows Event Viewer** and examine recent entries.*

Deployment in Medium to Large Infrastructure Environments

If an environment has two domain controllers, it is recommended to install the IDA software on each domain controller and set them up to monitor the local Windows Event Log.

In an environment with a larger infrastructure, there is no need to install the IDA software on every single domain controller. Instead, remote Windows Event Log monitoring should be enabled.

If there are multiple sites in different geographic locations, it is highly recommended to have the IDA software installed in each local network.

Important: The Windows Server event IDs must be correct

The D-Link IDA software will only listen for certain event IDs so the Windows Server should be configured so that the correct IDs are generated. The IDs that the IDA listens for are the following:

- ***103** - An RDP user has logged in and has been assigned a virtual IP.*
- ***104** - An RDP user has logged out and the user's IP has been released.*
- ***4624** - An account was successfully logged on.*
- ***4728** - Member added to global group.*
- ***4729** - Member removed from global group.*
- ***4756** - Member added to universal group.*
- ***4757** - Member removed from universal group.*
- ***4732** - A user has been added to a local domain group.*
- ***4733** - A user has been removed from a local domain group.*
- ***4768** - A user has logged in.*

Chapter 3: IDA Management

The IDA Management Interface

The IDA service listens for authenticated users and sends their details to the configured NetDefend Firewall. The IDA service has its own management user interface and this interface has a number of tabs which are described below.

- **The *General* tab**

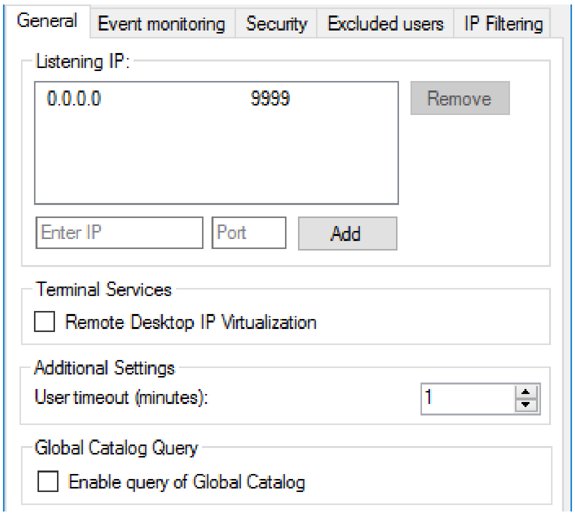
  This tab consists of the following settings:

  i. ***Listening IP*** - This is the IPv4 address and port number which the IDA will listen on for connections to NetDefendOS. By default, the IDA will listen on port *9999* of *0.0.0.0/0*, which means any IPv4 address. Multiple IP values can be entered for this setting and must include the IP configured for the NetDefendOS *Authentication Agent* object of the connecting firewall.

  ii. ***Remote Desktop IP Virtualization*** - This allows IDA to be used with a Windows Terminal Server™. This feature is described in detail later in this section.

  iii. ***User Timeout*** - This is the time within which NetDefendOS must authenticate the user after they are authenticated by the Windows server.

  iv. ***Global Catalog Query*** - By default, only the active directory is queried for the user. If this option is enabled and the active directory search fails then the global catalog will be queried.



Listening IP:

0.0.0.0 9999

Terminal Services

☐ Remote Desktop IP Virtualization

Additional Settings

User timeout (minutes): 1

Global Catalog Query

☐ Enable query of Global Catalog

Figure 3.1. The *General* Tab in the IDA Interface

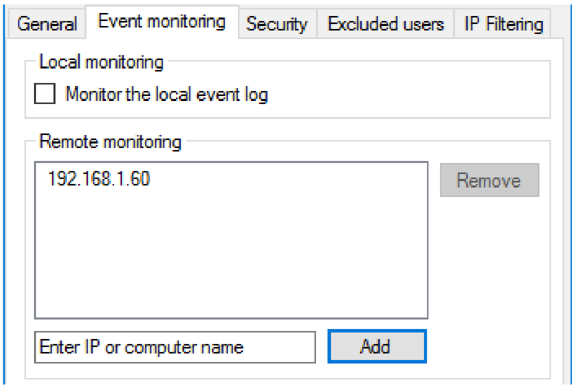
- **The *Event Monitoring* tab**

  This tab consists of the following settings:

  i. ***Monitor the local event log*** - When enabled, this IDA installation will monitor the server on which it is installed for authentication events. Usually, this will be enabled since normally the agent will monitor events on its own server.

  ii. ***Remote monitoring*** - This specifies the IP address of other domain servers which are to be monitored by this IDA installation. More than one IDA installation can monitor the same domain server and more than one IDA installation can send the same authentication event to NetDefendOS (duplicate received IDA events are recognized by NetDefendOS and ignored).

  If the *Monitor the local event log* option is not enabled and no other server IP addresses are specified, the agent will send nothing back to NetDefendOS.



Local monitoring

☐ Monitor the local event log

Remote monitoring

192.168.1.60

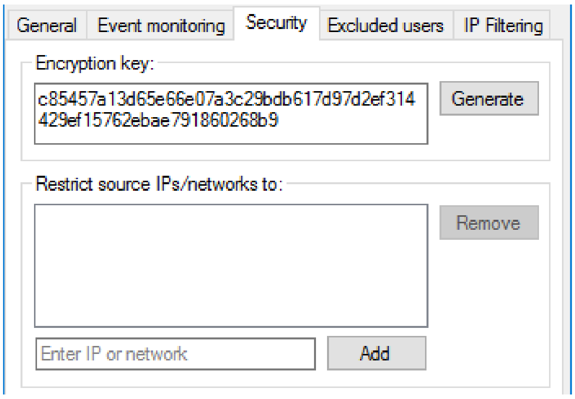
Figure 3.2. The *Event Monitoring* Tab in the IDA Interface

- **The *Security* tab**

  This tab consists of the following settings:

i. ***Encryption key*** - This is the key used to encrypt communication with NetDefendOS. By default, this value will be the same as the default value of the *Pre-Shared Key* property of the corresponding NetDefendOS *Authentication Agent* object. For improved security, it is recommended that this key is changed by the administrator, both for the IDA and the corresponding NetDefendOS *Authentication Agent* object.

ii. ***Restrict IPs/networks to*** - This specifies the source IPv4 addresses from which the IDA will accept NetDefendOS connections. By default, all IPv4 addresses will be accepted.



Encryption key:
c85457a13d65e66e07a3c29bdb617d97d2ef314429ef15762ebae791860268b9

Restrict source IPs/networks to:

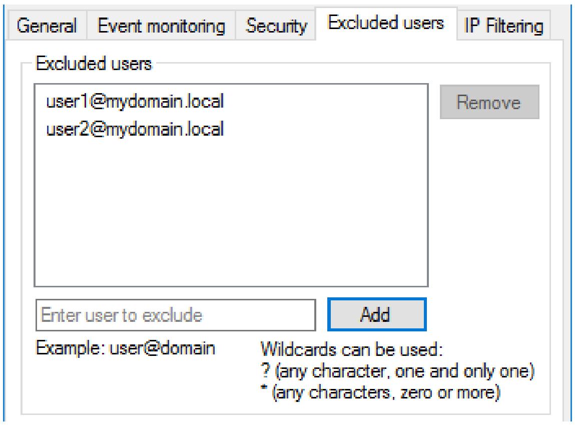
Figure 3.3. The *Security* Tab in the IDA Interface

- **The *Excluded Users* tab**

  In this tab, it is possible to set up an exclusion list for the IDA so that users on the list will not have their authentication status sent back to NetDefendOS by the IDA service. The full *User Principal Name* (UPN) must be used to specify excluded users, for example:

  ```
  myusername@mydomainname.local
  ```

  Often, it is appropriate to include the administrator's own account on this exclusion list.



Excluded users
user1@mydomain.local
user2@mydomain.local

Example: user@domain

Wildcards can be used:
? (any character, one and only one)
* (any characters, zero or more)

Figure 3.4. The *Excluded Users* Tab in the IDA Interface

When specifying excluded users, either or both of the following two wildcard characters can be used in any part of an address:

***** - An asterisk character can represent any character string. For example:

```
                   somename1@example.*
```

? - A question mark character can represent any single character. For example:

```
                   somename?@example.*
```

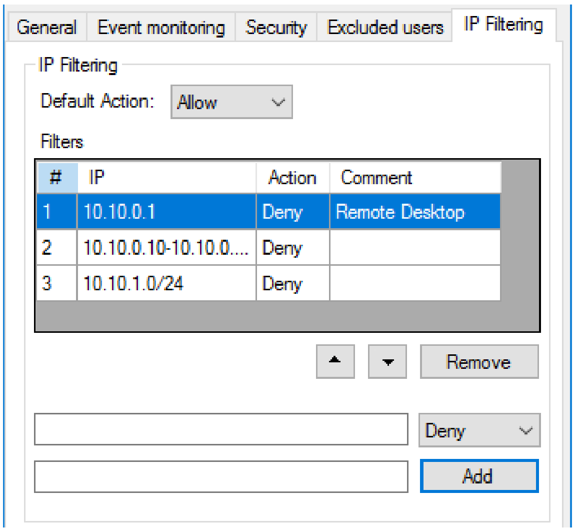
- **The *IP Filtering* tab**

  This tab allows the IP address of the authenticating client to be filtered using a list of filtering rules. Each rule added to the list by the administrator consists of an IP address, network or IP range, along with an action of either *Allow* or *Deny*.

  When the IDA processes a new client login, it scans the rule list from top to bottom and stops scanning at the first match for the client's IP address. If the action for the matching rule is *Allow*, the login is sent to NetDefendOS as normal. If the action is *Deny*, the login is ignored and no message is sent to NetDefendOS.

  If no match for the IP is found in the list, or the list is empty, the *Default Action* setting is applied. This setting is *Allow* by default.

  An empty list (the default) with the *Default Action* set to *Allow* means that all client IP addresses are allowed.



Default Action: Allow

#	IP	Action	Comment
1	10.10.0.1	Deny	Remote Desktop
2	10.10.0.10-10.10.0....	Deny	
3	10.10.1.0/24	Deny	

Figure 3.5. The *IP Filtering* Tab in the IDA Interface

An Example of IDA Redundancy

To illustrate how IDA redundancy could be implemented, consider a domain that has 4 servers called *A, B, C* and *D*. To implement minimal redundancy, the steps would be as follows:

1. Install the IDA on server *A* and server *B*.

2. Enable the *Event Monitoring* for both installations so they are monitoring local server authentication events.

3. For server *A*, configure the *Remote monitoring* option with the IP addresses of servers *B, C* and *D* so that they are monitored too.

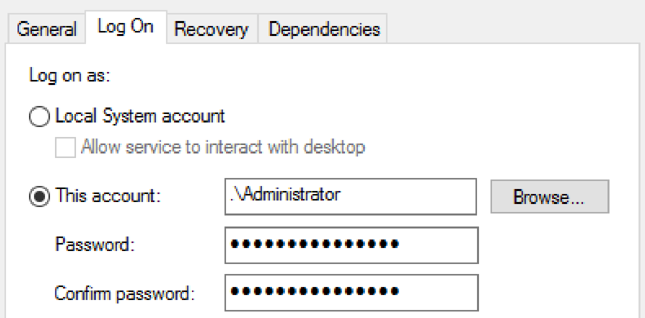
4. For server *B*, configure the *Remote monitoring* option with the IP addresses of servers *A, C* and *D* so that they are monitored too.

Now, if either server *A* or *B* should fail, authentication events will still be sent back to NetDefendOS. NetDefendOS will recognize any duplicate events sent by both server *A* and server *B*.

Using IDA with a Windows Terminal Server

In some environments, a *Terminal Server* may be used as well as a domain server. If this is the case, the IDA service is installed as before but the option *Remote Desktop IP Virtualization* should be enabled.

However, IP virtualization will not function with either Windows 2012 or 2016 Server if the IDA software is running as a *Local System account*. To solve this issue, change the settings in the *Log On* tab for the server to *This Account* and specify an account, as shown below:



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\Administrator

Password: •••••••••••••••

Confirm password: •••••••••••••••

Figure 3.6. Changing Windows 2012/16 Settings for IP Virtualization

The terminal server itself must have the following attributes:

- The role *Remote Desktop Session Host* must be installed.
- The option *IP virtualization per session* must be enabled.

Note: DNS lookup is done using the terminal server IP

Any DNS lookups are performed using the IP of the Windows terminal server and ***not*** *the session IP assigned to the client. Therefore, IP rules or IP policies may be needed to allow such DNS lookups through the firewall.*