Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Building 3
North London Business Park
Oakleigh Road South
London N11 1GN
United Kingdom

Tel: +44(0)20 3668 1580
Fax: +44(0)20 8446 3182
Web: www.deepnetsecurity.com
Email: support@deepnetsecurity.com
# Table of Contents

1 Introduction ............................................................................................................. 6

1.1 Platform Architecture ..................................................................................... 6  
   Web Access .......................................................................................................... 7  
   Cloud Access ....................................................................................................... 7  
   VPN Connection .................................................................................................. 7  
   Windows & Mac Logon ....................................................................................... 8  
   Outlook Anywhere & ActiveSync ................................................................. 8

1.2 Authentication Server Structure ..................................................................... 8  
   Identity Source .................................................................................................... 9  
   Domain ............................................................................................................... 10  
   Realm ............................................................................................................... 10  
   Application ....................................................................................................... 10  
   Agent ................................................................................................................. 10

2 Installation .......................................................................................................... 11

3 Quick Start ......................................................................................................... 11

4 Configuration ...................................................................................................... 12  
   4.1 Licenses ......................................................................................................... 12  
   4.2 Gateways....................................................................................................... 14  
   4.2.1 SMS Gateway .......................................................................................... 14  
   4.2.2 Email Gateway ........................................................................................ 15  
   4.2.3 Twitter Gateway ...................................................................................... 16  
   4.2.4 Telephone Gateway ............................................................................... 17  
   4.2.5 HTTP Proxy ........................................................................................... 18  
   4.3 Templates ...................................................................................................... 19

5 Identity Source ................................................................................................... 21  
   5.1 Create an Identity Source .............................................................................. 21  
   5.2 Modify an Identity Source .......................................................................... 25  
   5.3 Load Balancing ............................................................................................. 26

6 Domain ............................................................................................................... 28  
   6.1 Create a Domain .......................................................................................... 28

7 Realm .................................................................................................................. 29  
   7.1 Create a Realm ............................................................................................ 29  
   7.2 Manage Domains ......................................................................................... 29

8 Application ........................................................................................................ 30  
   8.1 Create an Application ................................................................................. 30
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2</td>
<td>Publish an Application</td>
<td>30</td>
</tr>
<tr>
<td>9</td>
<td>Logon Procedure</td>
<td>32</td>
</tr>
<tr>
<td>9.1</td>
<td>Create a Logon Procedure</td>
<td>32</td>
</tr>
<tr>
<td>9.2</td>
<td>Manage Logon Steps</td>
<td>32</td>
</tr>
<tr>
<td>9.2.1</td>
<td>Create a Logon Step</td>
<td>33</td>
</tr>
<tr>
<td>9.2.2</td>
<td>Sort Logon Steps</td>
<td>34</td>
</tr>
<tr>
<td>9.3</td>
<td>Assign a Logon Procedure</td>
<td>35</td>
</tr>
<tr>
<td>10</td>
<td>Agent</td>
<td>36</td>
</tr>
<tr>
<td>10.1</td>
<td>Register an Agent</td>
<td>36</td>
</tr>
<tr>
<td>10.2</td>
<td>Auto Registration</td>
<td>37</td>
</tr>
<tr>
<td>11</td>
<td>Policy</td>
<td>39</td>
</tr>
<tr>
<td>11.1</td>
<td>Manage Policies</td>
<td>40</td>
</tr>
<tr>
<td>11.2</td>
<td>Customise Policies</td>
<td>41</td>
</tr>
<tr>
<td>12</td>
<td>Roles</td>
<td>43</td>
</tr>
<tr>
<td>12.1</td>
<td>Manage Roles</td>
<td>44</td>
</tr>
<tr>
<td>12.2</td>
<td>Create Roles</td>
<td>44</td>
</tr>
<tr>
<td>12.3</td>
<td>Assign Roles</td>
<td>45</td>
</tr>
<tr>
<td>13</td>
<td>Token Management</td>
<td>46</td>
</tr>
<tr>
<td>13.1</td>
<td>Import Tokens</td>
<td>46</td>
</tr>
<tr>
<td>13.2</td>
<td>Assign Tokens</td>
<td>47</td>
</tr>
<tr>
<td>13.2.1</td>
<td>Single Assignment</td>
<td>47</td>
</tr>
<tr>
<td>13.2.2</td>
<td>Batch Assignment</td>
<td>48</td>
</tr>
<tr>
<td>13.3</td>
<td>Create Tokens</td>
<td>49</td>
</tr>
<tr>
<td>13.3.1</td>
<td>Single Creation</td>
<td>49</td>
</tr>
<tr>
<td>13.3.2</td>
<td>Batch Creation</td>
<td>50</td>
</tr>
<tr>
<td>13.4</td>
<td>Synchronise Tokens</td>
<td>51</td>
</tr>
<tr>
<td>13.5</td>
<td>Revoke Tokens</td>
<td>53</td>
</tr>
<tr>
<td>13.6</td>
<td>Delete Tokens</td>
<td>53</td>
</tr>
<tr>
<td>14</td>
<td>Token Provisioning</td>
<td>54</td>
</tr>
<tr>
<td>14.1</td>
<td>Configure a Provisioning Server</td>
<td>54</td>
</tr>
<tr>
<td>14.2</td>
<td>Provision Tokens</td>
<td>54</td>
</tr>
<tr>
<td>15</td>
<td>Auditing</td>
<td>55</td>
</tr>
<tr>
<td>15.1</td>
<td>Audit Configuration</td>
<td>55</td>
</tr>
<tr>
<td>15.2</td>
<td>Audit Viewer</td>
<td>55</td>
</tr>
<tr>
<td>15.3</td>
<td>Audit Monitor</td>
<td>56</td>
</tr>
<tr>
<td>15.4</td>
<td>Audit Export</td>
<td>57</td>
</tr>
</tbody>
</table>
16. Reporting ........................................................................................................................................58

16.1 Report Templates ....................................................................................................................58

16.2 Report Builder ........................................................................................................................58

17. Safe Mode .....................................................................................................................................61
1 Introduction

DualShield is a unified authentication platform that provides strong, mutual and multi-factor authentication services to all types of business applications, including VPN remote access, Web access, Cloud application, Windows Network Access and Windows Terminal Service. It supports a variety of authentication methods ranging from knowledge based password, on-demand password, one-time password, biometrics and certificate.

1.1 Platform Architecture

The entire DualShield platform consists of the following components:

- Authentication Server
- Management Console
- Single Sign-On (SSO) Server
- Self-Service Server
- Provisioning Server
- RADIUS Server
- Authentication Gateway
- IIS Agent
- VMWare View Agent
- Windows Agent
- Mac Agent

The core of the platform is the Authentication Server which manages user accounts and user credentials, and provides administration and authentication services. The DualShield authentication server is managed by the Management Console which provides a browser-based interface that is used by the system administrators to centrally manage the entire platform.

The platform provides various types of Authentication Agents that works with different types of business software applications, to provide the multi-factor authentication service.

Web Access

The Web Access authentication is provided by either the IIS Agent or the Authentication Gateway depending on the type of the web server. The IIS Agent adds a multi-factor authentication layer to the Microsoft IIS web server, protecting any application running on IIS such as Outlook Web Access, Sharepoint portals, Citrix Web Interface, Remote Desktop Web. The Authentication Gateway can be used to protect any type of web applications with multi-factor authentication, such as Citrix Access Gateway and SSL VPN devices.

Cloud Access

DualShield SSO Server is a SAML 2.0 compliant Identity Provider (IdP) that provides multi-factor authentication functions to web and cloud applications that support SAML 2.0 authentication protocol, such as Google Apps, SalesForce and Juniper SSL VPN appliances.

VPN Connection

Both the traditional IPSec VPN and the modern SSL VPN gateway and appliances support RADIUS authentication protocol. The DualShield platform comes with a RADIUS server that provides two-factor authentication for VPN access.

For IPSec VPN, only one-time password can be supported via RADIUS protocol because of the limitation in the RADIUS protocol. Advanced authentication methods such as Device DNA (DevicePass), keystroke dynamics (TypeSense) and voice and face recognition cannot be supported.

For SSL VPN, however, all types of authentication methods can be provided. For SSL VPN devices that support SAML 2.0, they can be configured to use DualShield Single Sign-On (SSO) Server as the Identity Provider to provide multi-factor authentication. For SSL VPN devices that do not support SAML 2.0, the DualShield Authentication Gateway can be used to control the access to the VPN service and to add multi-factor authentication.
Windows & Mac Logon

To add multi-factor authentication to the Windows and Mac logon, DualShield platform provides a Windows Logon Agent. This agent software can be installed on any Windows server machine in the network. In addition, DualShield platform also provides a Logon Client for the Windows and Mac workstations or PCs. This client software needs to be installed on the workstations or PCs if the users are required to authenticate with multi-factors.

Outlook Anywhere & ActiveSync

To add multi-factor authentication to Outlook Anywhere, DualShield platform provides an Authentication Client for the Outlook Anywhere application. This client software needs only to be installed on the desktop or laptop machine where the outlook client is running.

1.2 Authentication Server Structure

The authentication server consists of many components. To get started, you will need to understand the following key components and their relationships:

- Identity Source
- Domain
- Realm
- Application
- Agent

As illustrated in the diagram below:
Identity Source

An Identity Source is a user database or directory that stores all the users and identity data. Identity sources allow user and group information to be referenced in the location where your organization maintains it. For instance, if your organization keeps user data in a AD or LDAP directory, then you can add your AD or LDAP directory as an Identity Source into the DualShield authentication server. DualShield retrieves data from identity sources in real time and references data in one single source, therefore data is not synchronized or copied.
Domain

A domain is equivalent to an organization. A domain component itself does not store users’ identity data. Instead, a domain must be linked to an Identity Source which serves as the data store for the domain.

The relationship between domain and identity source is many-to-one (N→1), which means that one domain can only be connected to one identity source, but multiple domains can be connected to the same identity source.

Realm

A realm is a logical component that is used to organise domains. Multiple domains can be grouped into one realm, for the purpose of allowing users from different domains to access one single application. In a simple term, a realm is simply a group of domains.

The relationship between realm and domain is many-to-many (N→N), which means that one realm can contains many domain, and one domain can be connected to many realms.

Application

An application in the DualShield authentication server is an equivalent to a business software application, such as a VPN system, an Outlook Web Access or a Web portal. An application must be connected to a realm, as the realm contains domains of users who will be allowed the access to the application.

The relationship between application and realm is many-to-one (N→1), which means that an application can only be connected to one realm, but many different applications can be connected to the same realm.

Agent

An Agent refers to a DualShield Authentication or Administration Agent, such as:

- A DualShield Radius Server
- A DualShield Single Sign-On Server
- A DualShield Windows Logon Agent
- A DualShield Provisioning Server
- A DualShield Management Server
- A DualShield Self-Service Server

In order to allow users access to an application, the application has to be published by agents.

The relationship between Agent and Application is Many-To-Many, which means that one Agent can publish multiple applications and one application can be published in many different agents.
2 Installation

For the instruction of installing the DualShield platform software, please refer to the document:

DualShield Authentication Platform – Installation Guide.PDF

3 Quick Start

To get quick started, please refer to the document below:

DualShield Authentication Platform – Quick Start Guide.PDF
4 Configuration

4.1 Licenses

DualShield requires that a valid license key be installed on the system. Multiple license keys can be installed in one single server. To view the list of license keys that you have installed, click “Configuration | Licence”

To install a license key, the machine where DualShield is installed must have access to the Internet. If you need to a HTTP proxy for the Internet access, please refer to chapter 4.2.5 for the instruction of configuring the HTTP proxy.

To install a new license key, click “Import” button:

Enter your license key in the “Licence Key” field.

If there is no Internet connection from the server machine, you need to obtain your license data from the licensing server. Find a machine that has Internet connection, enter the URL below in your browser:

http://license.deepnetsecurity.com/register/install-license.htm
Enter the License Installation Code displayed on the management console. You will shortly receive your license data key in your email box.

Back to the management console. In the “Import Licence” window, select “Licence Data” from the “Input” field, then enter the license data that you just received. Click “Save” to save it.
4.2 Gateways

DualShield supports multiple communication gateways of various channels including SMS, email, telephone and twitter direct message.

To create a gateway, select “Configuration | Gateways” and click “Create” on the toolbar.

Select the gateway type from the “Type” list.

4.2.1 SMS Gateway

If you are planning to deploy tokens or send notification messages to your users via SMS text, then you need a SMS gateway. You can set up your own SMS gateway with a GSM modem or you might want to subscribe to a web-based SMS gateway service such as Clickatell.com.

Select “SMS” from the “Type” list.

Enter the name for the gateway to be created.

Select one or many domains from the “Domain” list. An application in DualShield can have its own gateway that is separate from other applications.

Click “Edit” to configure the gateway settings.
In the “Provider” dropdown list, select the SMS gateway service provider that you wish to use. Every SMS service provider has a different set of API, and DualShield provides a list of well-known providers in the installation. If your SMS service provider is not in the list, please contact Deepnet Support for the instruction of how to add it in to the list.

4.2.2 Email Gateway

If you are planning to deploy tokens or send notification messages to your users via email, then you need an email (SMTP) gateway.

Select “EMAIL” from the “Type” list
4.2.3 Twitter Gateway

DualShield also supports sending one-time passwords and other types of messages via Twitter direct message. A Twitter direct message is a peer to peer personal message that is private between the sender and receiver. You will need to register a Twitter account for your organisation and register the account details in your DualShield server.

Select “TWITTER” from the “Type” list

You can obtain the variables required in the form from your Twitter account.

1. Login into Twitter account
2. Click the “API” link on the bottom
3. Click the “Create an app” link in the page
4. Complete the application form

5. Submit the form
6. Click “My Applications” link
7. Click “Settings” tab
8. Look for “Application Type”

![Application Type](image)

9. Select “Read and Write”

10. Click the “Update Settings” button

11. Click “Details” tab

12. You can have the variables:

![OAuth settings](image)

**Note:** Users who wish to receive Twitter messages sent from DualShield must have their own personal Twitter accounts, and must follow the Twitter account that you have registered for your organisation.

### 4.2.4 Telephone Gateway

DualShield also supports sending one-time passwords and other types of messages via phone calls. Currently, the only telephone service provider supported by DualShield is TeleSign. If you plan to use TeleSign service, you will need to register an account directly with TeleSign.com.

Select “TELEPHONE” from the “Type” list
You must provide your user name, password as well as the variables below:

- customer_id
- api_key

### 4.2.5 HTTP Proxy

If the machine where DualShield is installed needs to access the Internet via a HTTP proxy, you must set up the HTTP proxy.

Select “HTTP” from the “Type” list
4.3 Templates

You can customise the messages that DualShield sends out to users by changing the message templates.

A template contains the following messages:

- One-Time Password
- Push Token
- Activation Code
- Authorisation Code
- Emergency Code

**One-Time Password**

When users are using the On-Demand password, T-Pass, DualShield sends out a one-time password to the user whenever it is needed or requested. This template defines the text of the one-time password message.

**Push Token**

Push Token means that DualShield server pushes a MobileID client and/or token to the user by sending a download message. It can be a manual push by the system administrator or an automatic push by DualShield server depending on the MobileID provisioning polices.

**Activation Code**

The activation code is used by users to activate their MobileID tokens in their account in the DualShield server. Depending on the MobileID policy, a user might or might not be required to activate their tokens.

**Authorisation Code**

The authorisation code is used by users to download their MobileID tokens from the DualShield server to their MobileID clients. Depending on the MobileID policy, a user might or might not be required to when downloading their tokens.

**Emergency Code**

This template defines the text of the emergency code message.

DualShield supports multiple message templates. Each domain can have its own template, allowing you to customise messages for different domains.

To create a message template, click “Configuration | Templates”, then click “Create” button on the toolbar in the Template Viewer window.
To bind a message template to one or many domains, select the template and click the context menu icon, then select “Domains” in the menu:

Select the domains to that the template will be assigned.

To customise messages in a template, select the template and click the context menu icon, then select “Messages” and the message to be customised in the menu:
5 Identity Source

After you have installed and configured your DualShield server, the next step is to add an Identity Source that holds your user accounts.

An Identity Source is a user database or directory that stores all the users and identity data. Identity sources allow user and group information to be referenced in the location where your organization maintains it. For instance, if your organization keeps user data in an AD or LDAP directory, then you can add your AD or LDAP directory as an Identity Source into the DualShield authentication server. DualShield retrieves data from identity sources in real time and references data in one single source, therefore data is not synchronized or copied.

Identity Source is the fundamental data component for building up the entire system. An identity source can be internal or external. An internal identity source uses the SQL database as its data store, and must be created from the ground up. An external identity source is linked to an existing AD or LDAP directory.

5.1 Create an Identity Source

To create an identity source,

- select “Identity | Identity Source” from the main menu
- click “Create” button in the toolbar

The Identity Source Creation Wizard is launched:
5.2 Modify an Identity Source

To modify an existing Identity Source, click the context menu icon (the down arrow) of the identity source you wish to modify and select “Edit”

One of the common changes that you might need to make to an external identity source is to add the dial prefix. If the telephone numbers stored in your identity source is not in the international format that includes country code, then you must add the dial prefix.

In some countries, local phone numbers start with zero (0). When converting local numbers to the international format by prefixing them with the country code, you need to remove the leading zero from the local numbers. The syntax for replacing a leading digit with a country code is:

Country Code|Leading Digit

For instance, “0044|0” will convert 079 7123 4567 to 0044 79 7123 4567
5.3 Load Balancing

If an identity source is an AD/LDAP directory and there are multiple servers in your network that serve the same AD/LDAP directory, then you might want to link the identity source in DualShield to some or all of those AD/LDAP servers to create a load balancing cluster.

To create or manage the load balancing cluster for an Identity Source, click the context menu icon of the identity source and select “LDAP Connections”

Click “Create” button in the toolbar to add a new AD/LDAP server.
You must assign a weight to every AD/LDAP server in the load balancing cluster. DualShield distributes traffic to all active servers in the cluster according to their weights. A server with a higher weight will get more traffic than a server with a lower weight.
6 Domain

While an Identity Source is a physical component that stores a database of user accounts and their identities, a domain is a logical component that is equivalent to the structure of an organization. A domain component itself does not store users’ identity data. Instead, a domain must be linked to an Identity Source which serves as the data store for the domain.

The relationship between domain and identity source is many-to-one (N→1), which means that one domain can only be connected to one identity source, but multiple domains can be connected to one identity source.

6.1 Create a Domain

To create a domain,

- select “Directory | Domains” from the main menu
- click “Create” button in the toolbar

The Domain Creation window is displayed:

Identity Source
Providing the user directory for the domain to be created.

Name
Providing a descriptive name of the domain.

DNS Name
Providing the Fully Qualified Domain Name (FQDN) of the domain. DNS Name is used by the IIS Agent for web applications.

NetBios Name
Providing the host or machine name of the domain. NetBios name is used by the Windows Agent for Windows logon.
7 Realm

A realm is a logical component that is used to organise domains. Multiple domains can be grouped into one realm, for the purpose of allowing users from different domains to access one single application. In a simple term, a realm is simply a group of domains.

The relationship between realm and domain is many-to-many (N→N), which means that one realm can contain many domains, and one domain can be included in many realms.

7.1 Create a Realm

To create a realm,

- Select “Authentication | Realms” from the main menu
- Click “Create” button in the toolbar
- Enter the “Name”
- Click “Save”

7.2 Manage Domains

To manage domains in a realm, e.g. add and/or remove, click the context menu of a realm and select “Domains”:

You can add a domain to the realm by selecting it, or remove a domain from the realm by unselecting it.
8 Application

An application in the DualShield authentication server is equivalent to a business software application, such as a VPN remote access, an Outlook Web Access or a SharePoint Web portal. It is important to note that a DualShield application can be used by one or shared by many software applications. For instance, you can have an application in DualShield that is shared by both OWA and SharePoint application.

An application must be connected to a realm, as the realm contains domains of users who will be allowed the access to the application. The relationship between application and realm is many-to-one (N→1), which means that an application can only be connected to one realm, but many different applications can be connected to one realm.

8.1 Create an Application

To create an application,

- Select “Authentication | Applications” from the main menu
- Click “Create” button in the toolbar
- Enter the “Name”
- Select a realm from the list
- Click “Save”

8.2 Publish an Application

An application must be published so that it can be accessed by users. Before an application is published, however, it must be assigned with a logon procedure that defines the how users will be authenticated in order to gain access to the application. Please refer to Chapter 9 for instruction of creating and managing logon procedure.

An application is published through an authentication agent. For instruction of creating and managing agents, please refer to Chapter 10.

To publish an application, select the application and click “Agents” in its context menu.
Select the agent in that the application will be published and click “Save”.
9 Logon Procedure

A logon procedure defines how users will be authenticated and what credentials users can used to authenticate themselves. Different applications might require different logon procedures, as they might have different security requirements.

A logon procedure consists of one or more logon steps. In a logon step, you define authentication methods or tokens that users will use to authenticate themselves. In other words, a logon procedure consists of a sequence of logon steps, and a logon steps consists of a set of logon methods.

9.1 Create a Logon Procedure

To create a logon procedure,

- Select “Authentication | Logon Procedure” from the main menu
- Click “Create” on the toolbar

There are 3 types of logon procedure that you can select,

- Windows
- RADIUS
- Web SSO

“Windows” is for Windows Logon, “Web SSO” is for any web and cloud application and “RADIUS” is for any RADIUS based application.

9.2 Manage Logon Steps

To manage logon steps in a logon procedure,

- Select the logon procedure and click its context menu
- Select “logon steps” in the context menu
9.2.1 Create a Logon Step

To create a new logon step, click the “Create” button on the toolbar.
Select the authenticators you need for this logon step and click “Save”.

If you selected the “Challenge & Response” option, the users will be required to authenticate in a challenge and response mode in which users will be prompted with a challenge code and asked to enter a response code. Only MobileID and SafeID Pinpad tokens support challenge and response function.

### 9.2.2 Sort Logon Steps

[Diagram of Logon Step View]
9.3 Assign a Logon Procedure

An application in DualShield must be assigned with a logon procedure of the right type. If a DualShield application is designed for Web-based software applications, then it must be assigned with a logon procedure in the type of “Web SSO”, for instance.

As we know, a DualShield application can be used by one or many software applications of the same type or even different types. If a DualShield application is shared by several software applications of different types, then you must assign a logon procedure of each type to the application. In other words, a DualShield application can have multiple logon procedures of different types. However, a DualShield application must not be assigned with more than one logon procedure of the same type.

To assign a logon procedure to an application,

- Select the logon procedure to be assigned
- Click the context menu icon of the Logon Procedure
- Select “Applications” in the context menu

A list of all applications will be displayed:

- Select the applications to that you want to assign the logon procedure.
10 Agent

An Agent can be a DualShield Authentication or Administration Agent, such as:

- A DualShield Radius Server
- A DualShield Single Sign-On Server
- A DualShield Provisioning Server
- A DualShield Management Console
- A DualShield Self-Service Console
- A DualShield Windows Logon Agent
- A DualShield VMWare View Agent

Authentication agents are software applications that securely pass user authentication requests to and from DualShield Authentication Server.

To enable an authentication agent to pass authentication requests to DualShield Authentication Server, you must do the following:

- Install an authentication agent on each machine you want to protect with the DualShield Authentication Server. See the agent installation guide.
- Use the DualShield Management Console to add a record for the new agent to the internal database. The agent record identifies the agent to Authentication Server. This process is known as registering the agent.
- Use the Management Console to generate an Agent Configuration File for the agent. This allows the agent to locate Authentication Server and communicate with the Authentication Server via HTTPS/SSL protocol.

10.1 Register an Agent

Registering an agent is normally a part of the installation process of the agent software.

To register an agent,

- select “Authentication | Agents” from the main menu
- click “Register” button in the toolbar
Agent IP Address
Providing the IP address of the machine where the Agent has been or is being installed.

Agent Public URL
Some agents such as the Provisioning Server are to be accessed by end users, therefore requires a public Internet address (URL).

Certificate Password
DualShield automatically creates a certificate the agent. A password is required for the protection of the certificate.

Agent Data
Containing the information about the agent. It will be provided by the agent installer.

10.2 Auto Registration
Some agents have an installation program that is capable of registering itself with the authentication server. For the security purpose, however, the auto registration function in the authentication server is disabled by default.

To turn on auto registration,

- select “Authentication | Agents” from the main menu
- click “Auto Registration” button in the toolbar
Select “Enabled” to enable auto registration.

Optionally, you can specify the time period in which auto registration will be enabled.

For extra security, you can also select “Check IP” and enter the IP addresses so that the authentication server will check the agent’s IP address and only allow the agent whose IP address is in the specified IP addresses.
11 Policy

The DualShield platform is controlled by various types of polices. At the installation, DualShield provides a default policy of each policy category. These default polices are system level policies and applied to the entire system. You can accept the default policies or create custom policies and apply them to the desired objects and elements.

You can use the following policies to help administer your system:

Access Control
Access Control policies define days and hours in which a user can access a specified application.

Access Control - IP
Access Control - IP policies define IP addresses of the machines from which a user can access a specified application.

Activation
Activation policy defines how an authentication product/token will be activated. Different product may be activated in different ways, therefore each product has its own activation policy. Activation Policy is not a top-level policy category; it is an option in a product’s policy.

Activation Code
Activation Code is sent by the server to users, and used by users to activate tokens in their user accounts. The policy defines the construction and lifespan of an activation code, such as the length, validity and characters of the code.

Authorization Code
Authorization Code is sent by the server to users, and used by users to activate MobileID tokens downloaded into their Mobile devices. The policy defines the construction and lifespan of an activation code, such as the length and characters of the code.

Challenge Code
Some authentication products such as MobileID, GridID etc support challenge and response. The construction of the challenge code is product dependant therefore not configurable. However, the lifespan of the Challenge Code is configurable by the Challenge Code policy.

Emergency Code
In the case when a user has lost or misplaced their tokens and needs to access an application protected with two-factor authentication urgently. An emergency code can be issued to temporarily replace the user’s token. The policy defines the construction and lifespan of an activation code, such as the length and characters of the code.

Logon
Logon polices define whether a user or a group of users is mandated to logon with two-factor authentication, or whether they can logon to a two-factor enabled application without having to authenticate with two factors.
Lockout
Lockout policies define how many failed logon attempts users can make before the system locks their accounts.

Offline
The offline policy is only applicable to Windows logon. The policy defines whether or not two-factor authentication is required when users attempt to login to their machines that are offline.

Provisioning
Provisioning policy defines how an authentication product/token will be provisioned. Different product may be provisioned in different ways therefore each product has its own provisioning policy. Provisioning Policy is not a top-level policy category; it is an option in a product’s policy.

Session
Session policies define the lifetime and timeout values of the Management Console.

Static Password
Static Password policies define users' password length, format, and frequency of change etc.

Every authentication product, e.g. MobileID, T-Pass, etc. has their own policy settings therefore there is a policy for each of the product.

Other Deepnet products that you install may add additional policy types.

11.1 Manage Policies
To manage your policies, select “Administration| Policies” from the main menu:

On the left side is the policy search pane. You can search polices by their category and/or holders.
11.2 Customise Policies

At the installation, DualShield generates a default policy of each policy type/category. These default policies are system level policies and applied to the entire system. You can accept the default policies or create custom policies and apply them to the desired objects or elements.

Before you create custom policies, you need to understand the following rules:

1. A policy always has a holder or owner. The holder of the default system policies is the system itself.

2. There are 6 types of policy holders:
   1) System
   2) Domain
   3) Unit
   4) Group
   5) Users

3. When DualShield searches for a policy, it starts from the bottom of the above holder list. If it finds the required policy, it stops the search. Effectively, a policy is inherited from “parent” holder unless the policy is defined by the holder itself. For instance, when searching for a user’s logon policy for a specific application, DualShield starts from the user’s logon policy that is associated with the application that the user is attempting to access. If found then DualShield stops search and use the user’s logon policy. If the user does not have his/her own logon policy, DualShield goes up one level and check if the groups that user belongs to have logon policies for the application that the user is attempting to access. And so on.

4. A user may be a member of several groups. When search a policy on the group level, DualShield merges the policy attributes of all groups that the user belongs to. If there are conflicts found in an attribute, DualShield will go up the list and search the attribute in the user’s unit policy, or domain or system policy.

To create a custom policy, you can either create a new policy or clone from an existing policy.

Clone and Customise:

- Find an existing policy, such as the system policy
- Click the context menu icon of the policy
- Select “Clone”
Select the Destination Holder, and Domain, Group, Unit, User if applicable.

Select the applications to that you want to apply this policy, if applicable.
12 Roles

DualShield employs the Role Based Access Control (RBAC) model for access control to the Management Console.

- A user belongs to or has one or many roles
- A role has a set of access permissions
- A permission is right to execution or access

An administrative role is a collection of permissions that can be assigned to an administrator. A role determines what level of control the administrator has over which objects, such as users, user groups, and so on.

You can add as many custom administrative roles as your organization needs. You can also assign multiple roles to a single administrator. When an administrator has more than one role, the privileges granted by those roles are combined, allowing the administrator to perform any action granted by the assigned roles.

For example, suppose an administrator is assigned one role that grants permission to view and edit users, and another role that grants permissions to view and edit user groups. Each time the administrator logs on, he or she can view and edit both users and user groups.

A role has 3 properties:
- A descriptive name
- A set of managing domains
- A collection of permissions based on the function of the role

A permission has 3 components:
- A set of scopes
- A set of objects
- A set of actions

The managing domains of an administrative role determine the domains in which the role lives and is managed (by other administrative users with the right to manage roles).

The scope of an administrative role determines in what scope administrator may manage objects.

Actions assigned to the administrative role determine what actions an administrator assigned the role can take on objects such as users, user groups, security domain, units, and various policies. The following common privileges are available for all objects:

1. **All** grants an administrator permission to perform any administrative action on the object.
2. **Create** grants an administrator permission to create/add an object.
3. **Delete** grants an administrator permission to delete an object.
4. **Edit** grants an administrator permission to view and edit an object, but not the ability to create or delete.
5. View grants an administrator permission to view an object, but not the ability to add, edit, or delete.

Each object may also have its own special privileges.

You can only assign and add administrative roles with the same or fewer objects than the administrative role assigned to you.

You can only assign and add administrative roles with the same or fewer privileges than the administrative role assigned to you.

12.1 Manage Roles

To manage roles, select “Administration | Roles” to open the role manager.

There are several predefined roles which can be edited but not deleted.

12.2 Create Roles

To create a new role, click the “Create” button on the toolbar.

You can select the managing domains for this role, or you can leave it empty. If you do select managing domains, then this role can only be managed by administrative users in the selected domains who have the right to manage roles. If you do not select managing domains, then this role can be managed by all administrative users who have the right to manage roles.

Once a role is created, you will then need to give it some permits. A role can have a collection of permits. To edit a role’s permits, select the role, click its context menu and select “Permits”.
To create a new permit, click the “Create” button on the toolbar.

Select “Scope”, “Object” and “Actions”, and press “Save” to save it.

### 12.3 Assign Roles

To assign roles to a user, find the user account in the user manager. Select the user, click its context menu. Select “Assigned Roles” in the context menu:

Select the roles you wish to assign to the user.
13 Token Management

DualShield provides a central place where the system administrators can centrally manage all tokens in the entire system, Token Repository. For extra flexibility and security, the system administrators can create multiple token repositories, sub repositories within a repository, and bind a repository to a domain, group or a unit. This allows domain/group/unit administrators to manage only tokens that are allocated to their domains, groups or units.

From within the Token Management facility the administrators can manage the full life cycle of tokens such as assigning tokens to users, synchronising tokens, importing new tokens or deleting existing tokens.

13.1 Import Tokens

Hardware tokens must be first imported into the system before they can be assigned to users. The process of importing hardware tokens involves importing a so-called token seed file. A single seed file can contain information of one or many tokens.

To import tokens, follow the steps below.

1. In the main menu, select “Repository | Token Management”.
2. On the left pane, select the token repository where you want to place the new tokens.
3. On the right pane, press the “Import” button on the toolbar.
4. Click the File Browser button to the right of the Token Seed File box and select the token seed file to be imported.
5. Optionally, enter the password if the token seed file is encrypted.
6. Click the “Import” to start the import process.

13.2 Assign Tokens

You can assign one token to a user at a time (single assignment) or a number of tokens to each of its user at a time (batch assignment).

13.2.1 Single Assignment

To assign one token to a user, follow the steps below:

1. Locate and select the token you wish to assign in the token repository
2. Click the context menu of the token
3. Click “Assignment” in the context menu

4. Click “New Assignment” on the toolbar
5. Select the Domain in which the user resides
6. Enter the user’s login name or use the search button to search the user in the domain
7. Optionally, you can specify the start, expiration date/time of the assignment, and/or the usage limit of the token by this user.
8. Click “Assign” button to finish the assignment.

13.2.2 Batch Assignment

To assign a number of tokens in one single operation, you will first need to create a CSV (Comma Separated Values) file, then use the “Assign Tokens” feature which is located on the toolbar in the Token Management view.

CSV is a delimited data format that has fields/columns separated by the comma character and records/rows terminated by newlines. Fields that contain a special character (comma, newline, or double quote), must be enclosed in double quotes. If a line contains a single entry which is the empty string, it may be enclosed in double quotes. If a field’s value contains a double quote character it is escaped by placing another double quote character next to it.

The first line in a csv file must contain column names in each of the fields. The column names for the token batch assignment are:

- domain
- loginName
- manufacturerCode
- productCode
- serial

Note that column names are case sensitive.

<table>
<thead>
<tr>
<th>column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>The name of the domain in which the user resides</td>
</tr>
<tr>
<td>loginName</td>
<td>The user’s login name</td>
</tr>
<tr>
<td>manufacturerCode</td>
<td>The manufacturer code of the token. Tokens produced by Deepnet Security has the manufacturer code: DN</td>
</tr>
</tbody>
</table>
**productCode:** The product code of the token. Tokens produced by Deepnet Security have the following codes:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE</td>
<td>SafeID, Event-Based</td>
</tr>
<tr>
<td>ST</td>
<td>SafeID, Time-Based</td>
</tr>
</tbody>
</table>

**serial:** The serial number of the token

Example:

```
<table>
<thead>
<tr>
<th>domain, loginName, manufacturerCode, productCode, serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;deepnetsecurity.com&quot;, &quot;john.smith&quot;, DN, ST, 20001001</td>
</tr>
<tr>
<td>&quot;deepnetsecurity.com&quot;, &quot;joe.bloggs&quot;, DN, SE, 10001002</td>
</tr>
</tbody>
</table>
```

The above CSV file will assign two tokens:

1. A Deepnet SafeID (Time Based) token with the serial number 20001001 to a user with the login name “john.smith” in the domain “deepnetsecurity.com”
2. A Deepnet SafeID (Event Based) token with the serial number 10001002 to a user with the login name “joe.bloggs” in the domain “deepnetsecurity.com”

### 13.3 Create Tokens

While hardware tokens have to be first imported into the system then assigned to users, software tokens such as MobileID can be simply created for the users.

Similarly, you can create one software token for a user at a time (single creation) or a software token for a number of users in a single operation (batch creation).

#### 13.3.1 Single Creation

To create one token for a user, follow the steps below:

1. Locate and select the user in the user directory
2. Click the context menu of the user
3. Select “Tokens” in the context menu
4. Click the “Create” button on the toolbar

5. Select the type of the token product you wish to create, e.g. MobileID/Time-Based

6. Optionally, provide the details of the token properties

7. Click the “Save” button to create the token

13.3.2 Batch Creation

You can create a soft token for all users in a group, a unit or an entire domain. This feature is called “Deploy Tokens”.

1. Locate the group, unit or the domain in the user directory

2. Click its context menu

3. Select “Deploy Tokens” in the context menu

4. Select the type of the token product you wish to deploy

5. Click the “Deploy” button to start the batch deployment process

Deploying tokens will be executed as a background task as it may take a length of time. You can check its progress in the Task list, and its result in the Audit trails.
13.4 Synchronise Tokens

One-time password tokens can be out of sync causing failure to login. For event/counter based OTP token, the most common cause of out-of-sync is that the user has generated too many dynamic passwords in the token device without using them. For time based OTP tokens, time drifts in the token device can cause a token to be out of sync with the server.

In DualShield you can pre-set a window in which tokens can be automatically synchronised by the server. However, when the counter or the clock in a token has drifted outside the pre-set window, the token has to be manually synchronised by the user or the system administrator.

The preset window values are configurable in the token’s policy settings.

Below are the default settings for SafeID Event-Based tokens:

![Policy Info -- Edit](image)

*Maximum steps in automatic synchronisation*
This value specifies the maximum steps that the server will look forward and backward in order to automatically re-synchronise the token.

*Maximum steps in manual synchronisation*
This value specifies the maximum steps that the server will look forward and backward in order to re-synchronise the token in the manual synchronisation the user.

*Maximum steps in checking synchronisation*
This value specifies the maximum steps that the server will look forward and backward in order to detect if a token is out of sync.
Below are the default settings for SafeID Time-Based tokens:

![Policy Info -- Edit]

**Maximum time windows in automatic synchronisation**
This value specifies the maximum windows that the server will look forward and backward in order to automatically re-synchronise the token.

**Maximum time windows in manual synchronisation**
This value specifies the maximum windows that the server will look forward and backward in order to re-synchronise the token in the manual synchronisation the user.

**Maximum time windows in checking synchronisation**
This value specifies the maximum windows that the server will look forward and backward in order to detect if a token is out of sync.

To synchronise a token in the Management Console, select “Synchronise” in the token’s context menu:

![Synchronise -- View]

Depending on the token’s policy settings, you will need to generate two or more OTPs from the token. Optionally, you can also enter a value in the Search Scope field to overwrite the token’s synchronisation policy setting: **Maximum steps/time windows in manual synchronisation**, which allows you to enlarge the search steps or windows.
13.5 Revoke Tokens

If a token is lost, damaged or becomes malfunctioned, you can temporarily disable the token or “decease” the token. Later, you can also re-enable it or “revive” the token. These functions are located in the context menu of the token.

13.6 Delete Tokens

You can also permanently remove a token from the server by deleting it.
14 Token Provisioning

DualShield provides several software tokens such as MobileID and T-Pass, and a provisioning server for provisioning those tokens to end users.

14.1 Configure a Provisioning Server

In a DualShield platform, you can install and register one or many provisioning servers. To the authentication server, a provisioning server is an agent. Therefore, provisioning servers are managed in the agent list.

A provisioning server provides services directly to the end-users, therefore it must be given a public or external Internet address, a URL, in the format below:

- if the provisioning server is operating in non-SSL mode
  
  http://fqdn-or-ip:port

- if the provisioning server is operating in the SSL mode

  https://fqdn-or-ip:port

When a provisioning server sends out token provisioning messages to users, it will include its public URL in the messages. Therefore, you must make sure that the public URL can be correctly resolved. Usually, you will need to map the external FQDN or IP to the internal IP address of the provisioning server, and the external port to the internal port of the provisioning server. By default, the internal port of the provisioning server is 8072.

To configure a provisioning server,

- select “Authentication | Agents” from the main menu
- select the provisioning server to be configured
- click “edit” in the context menu

14.2 Provision Tokens

Different types of authenticator or tokens are provisioned differently. Please refer to the administration guide of the authenticator/token (such as MobileID) for instructions.
15 Auditing

DualShield maintains logs of all system events. You can use these logs to monitor the system and maintain an audit trail of all logon requests and operations performed using the Management Console.

DualShield maintains the following logs:

- **Administrative.** Captures log messages that record any administrative action, such as adding and editing users.
- **Runtime.** Captures log messages that record any runtime activity, such as authentication of users.
- **System.** Captures log messages that record system level messages, such as connection to an AD server has failed.

DualShield can be configured to record every single event or selected events only.

15.1 Audit Configuration

To configure the audit log,

1. Select “Configuration | Audit”

2. Select the events that you wish to be logged

There are hundreds of events in the system. You can quick search for events by entering a keyword in the “Find Events” search box.

15.2 Audit Viewer

To view audit logs, select “Administration | Audit”
The Audit Viewer provides functions such as Zoom In, Auto Refresh and Export.

An event might consist of a list of sub-events. To see the list of sub-event of an event, select the event and click “Zoom In” button on the toolbar.

You can also check the details for each event by dragging up the Audit Details and Log Fields window on the bottom:

The Audit Details tab contains detailed information of an event

The Log Field tab contains detailed information of the API call

15.3 Audit Monitor

The Audit View also provides a very useful feature, Auto Refresh. In auto refresh mode, the viewer will automatically reload logs at the defined interval. Effectively, auto refresh turns the audit viewer into a live event monitor.
To turn on auto refresh, press down the “Start Auto Refresh” button. To define the auto refresh interval, click “Configure Auto Refresh”.

15.4 Audit Export

You can export audit logs and save as a CSV or XML file for the purpose of archiving or generating reports using third-party report tools.

To export, click the “Export” button:
16. Reporting

You can create and generate customized reports that describe system events or objects information, or produce statistic data. These reports can provide you with more detailed information on the events that occur within the system.

For example, you might want to create a report that shows you all of the user accounts that are disabled or locked. You can design the report so that it includes relevant information such as user name, domain and the number of tokens.

You might also want to create a report that shows administrator activities. You can use the report to view activities for all administrators or you can customize the report to display detailed information on one administrator. There are many reporting options available to you.

16.1 Report Templates

You can create custom reports from the predefined set of report templates. Each template includes a predefined set of input parameters, output columns, and options for formatting the result.

To view the list of report templates, select “Administration | Report”

![Report Templates Table]

New report templates are being added and published online. If the report template that you are looking for is not in the list, you can check it online, download and import it if it is available. To download report templates, click “Download” button on the toolbar. After a report template is downloaded and save in your hard disk, you will need to import it by clicking “Import” button.

16.2 Report Builder

To create a custom report, first select a template from the predefined list of templates. The template that you select is the foundation for your custom report. The template offers a starting point for sets of data, including input parameters and output columns. You can customize the report further by adding and removing input parameters and output columns, using the report builder.

To generate a report, click “Generate” in the context menu of the select template. This brings up the report builder.
In the report builder, we can build a query statement by adding input parameter. If we are going to generate a report that lists all logon attempts that failed, for instance, then we will build the following query statement:

```
eventCode equals 'Logon' and errorCode not equals 'succeeded'
```

To configure the output columns, click “configure output...” button.
You can specify the output file format, e.g. PDF, HTML, XML etc., and output columns.

Finally, to generate the report, click “Generate” button. Generating a report might take a while. While a report is being generated, you can close the report builder and leave it running in the background. As soon as a report is completed, it will be automatically downloaded.
17. Safe Mode

If the system administrators have forgotten their passwords and/or have lost their tokens, they will not be able to login to the authentication server. There is no master password whatsoever that could be used to gain access. The only way in is to restart the DualShield server in the so-called Safe Mode. The safe mode operation allows the system administrator to login without password or token. As soon as the administrator has reset their password in the safe mode, they must remove the safe mode switch and restart the DualShield server to the normal operation mode.

To switch on the Safe Mode, you will need to add the Safe Mode switch to the JVM runtime parameter list.

**On Windows,** launch “Regedit” and navigate to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\DualShield\Parameters\Java
```

Then edit the “Options” value, append “-Ddual.safe.mode=true” to the end of the value:

![Registry Editor](image)

Finally, restart the DualShield service:

```
net stop dualshield
net start dualshield
```
On LINUX, edit the file: `/etc/init.d/dualshield`, append `"-Ddual.safe.mode=true"` to the line:

```
CATALINA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=256m -Djava.awt.headless=true"
```

This will become:

```
CATALINA_OPTS="-Xms256m -Xmx1024m -XX:MaxPermSize=256m -Djava.awt.headless=true
-Ddual.safe.mode=true"
```

Finally, restart the DualShield service:

```
sudo /etc/init.d/dualshield stop
sudo /etc/init.d/dualshield start
```