
Setting up Deepnet for 2X VirtualDesktopServer or 2X ApplicationServer Manual



2X Software Ltd.





URL: www.2x.com

E-mail: info@2x.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of 2X SOFTWARE Ltd.

2X ApplicationServer and 2X VirtualDesktopServer are copyright of 2X SOFTWARE Ltd. © 1999-2009 2X SOFTWARE Ltd. All rights reserved.

Version 2.0 – Last updated September 1, 2009

Contents

Configure Deepnet	5
System Settings	5
Servers	5
Gateways.....	6
Templates.....	7
Applications	9
Token Repository.....	9
Configure 2X Server	10
List of Supported Tokens	10
Connect to Deepnet Unified Authentication	10
Creating User Accounts on Deepnet	15
Connect to a Terminal Server Connection	16
Connect to a Terminal Server Connection.....	16
2X Access Portal	18

CONFIGURE DEEPNET

Start by logging into the machine where Deepnet Unified Authentication is installed and open your internet browser. Since Deepnet is installed locally, use 'localhost' as the URL followed by the port number which the Deepnet server will use to communicate with your applications (ex: <http://localhost:8080/>).

You must then login in to the Deepnet Management Console with the credentials that you had set during the installation.

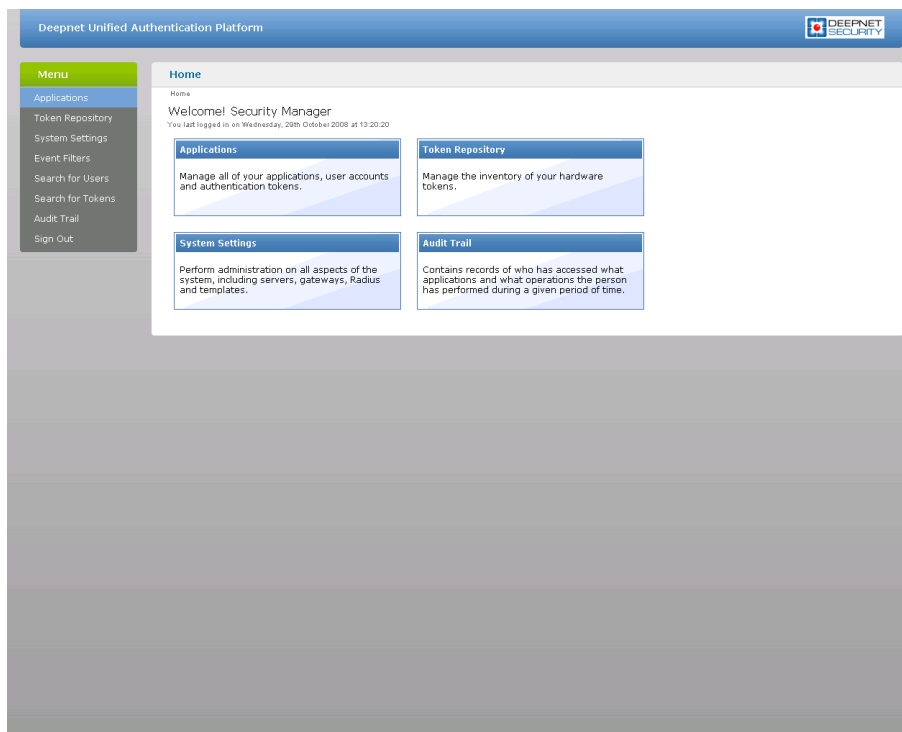


Figure 1: Deepnet Management Console

System Settings

Servers

Ensure that the Communication Server, Connection Server and Authentication Server are properly configured. For further information please refer to Deepnet Unified Authentication Platform Administration Guide.

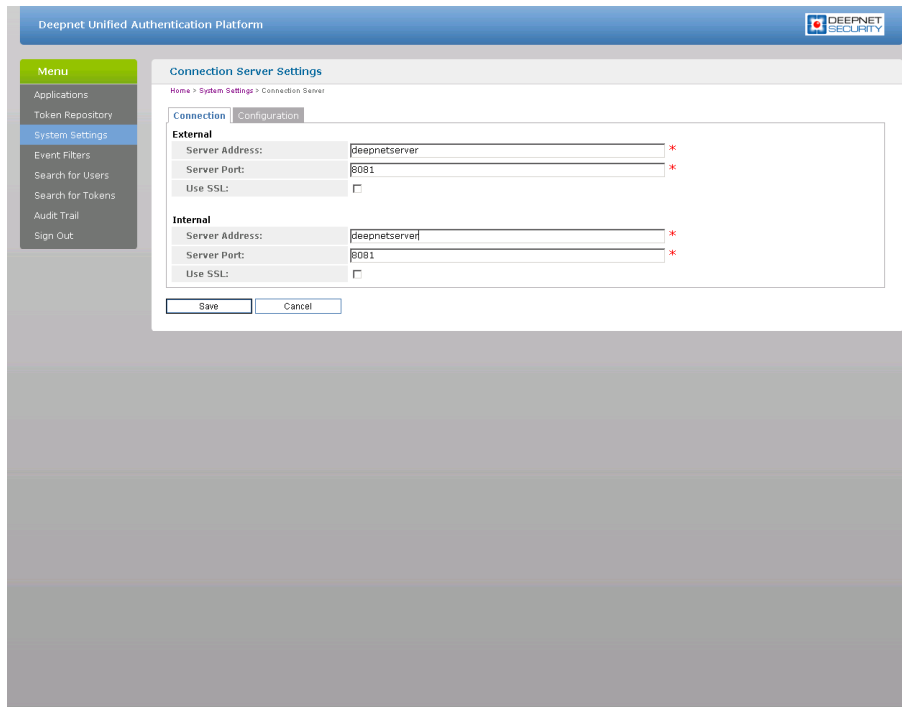


Figure 2: Connection Server settings

The 2X Publishing Agent will communicate with the Authentication Server. It is highly recommended to have this behind a Firewall for security reasons. Make sure that the 'Server Address' and 'Server Port' are correct.

Gateways

Email or SMS Gateways must be configured correctly so that the Deepnet server is able to send information, such as Activation codes, to the users.

The screenshot displays the 'Email Gateway Settings' page within the Deepnet Unified Authentication Platform. The interface includes a top navigation bar with the platform name and logo, and a left-hand menu with options like Applications, Token Repository, System Settings, Event Filters, Search for Users, Search for Tokens, Audit Trail, and Sign Out. The main content area is titled 'Email Gateway Settings' and contains a breadcrumb trail: 'Home > System Settings > Email Gateway Settings'. Below this, there are several input fields: 'SMTP Server Address' (containing '127.0.0.1'), 'SMTP Server Port' (containing '25'), 'Requires Authentication' (checkbox), 'Transport Layer Security (TLS)' (checkbox), 'User Name', and 'Password'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 3: E-Mail Gateway settings

The E-Mail Gateway and/or SMS Gateway must be configured to be able to send messages to the user. Enter the 'SMTP Server Address' and 'SMTP Server Port' of the server which will be used by the Deepnet Unified Authentication to send e-mails. Remember to enter any username or password used for the SMTP server.

Templates

Templates are used to set the structure of e-mails and SMS messages sent by the server.

The SMS template allows you to set the text for the 'Sender' field, the message content and an optional subject. Make sure that you use the preset wildcards to send unique information such as the One-Time Password ([[OTP]])

Deepnet Unified Authentication Platform DEEPNET SECURITY

Menu

- Applications
- Token Repository
- System Settings
- Event Filters
- Search for Users
- Search for Tokens
- Audit Trail
- Sign Out

Send One-time Password Templates

Home > System Settings > OTP Template

SMS Template | **SMTP Template**

From: *

Subject: *

Body:

(for One-Way OTP)

Your one-time password: *

(for Two-Way OTP)

Your one-time password: *

Server one-time password: *

Format: HTML Plain Text

Priority: Low Mid High

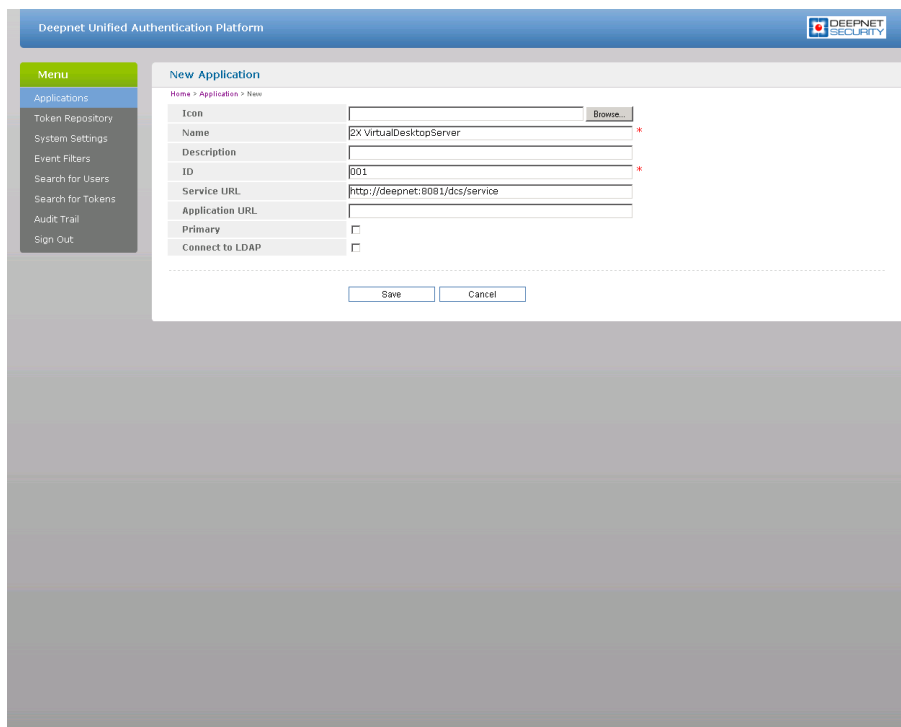
Note: Use the following wildcards:

- [[OTP]] : User's One-Time Password
- [[SOTP]] : Server's One-Time Password

Figure 4: One-Time Password Template

The E-mail template allows you to set the e-mail address that the user can reply to. This should be set to the administrator's e-mail. You can also set the e-mail's 'Subject', 'Priority' and 'Format'. The 'Body' contains the actual content of the e-mail which should include the preset wildcard for the unique information along with a message.

Applications



The screenshot shows the 'New Application' form in the Deepnet Unified Authentication Platform. The form is titled 'New Application' and has a breadcrumb trail 'Home > Application > New'. The form fields are as follows:

Field	Value
Icon	[Browse]
Name	2X VirtualDesktopServer *
Description	
ID	001 *
Service URL	http://deepnet:8081/dcs/service
Application URL	
Primary	<input type="checkbox"/>
Connect to LDAP	<input type="checkbox"/>

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Figure 5: Add a new application

Click on 'New' to add a new application. From the new form that loads you only need to set a 'Name' (ex: 2X Server) and an 'ID' (ex: 001). Once this is done, click 'Save' to save your settings.

Token Repository

If using hardware tokens such as SafeID the token information must first be imported using the XML file provided. Click on 'Import' and browse for the XML file provided. After the XML file has been imported each hardware token must be assigned to a user.

CONFIGURE 2X SERVER

List of Supported Tokens

- SafeID
- FlashID
- MobileID
- QuickID
- GridID
- SecureID (RSA)
- DigiPass (Vasco)

Connect to Deepnet Unified Authentication

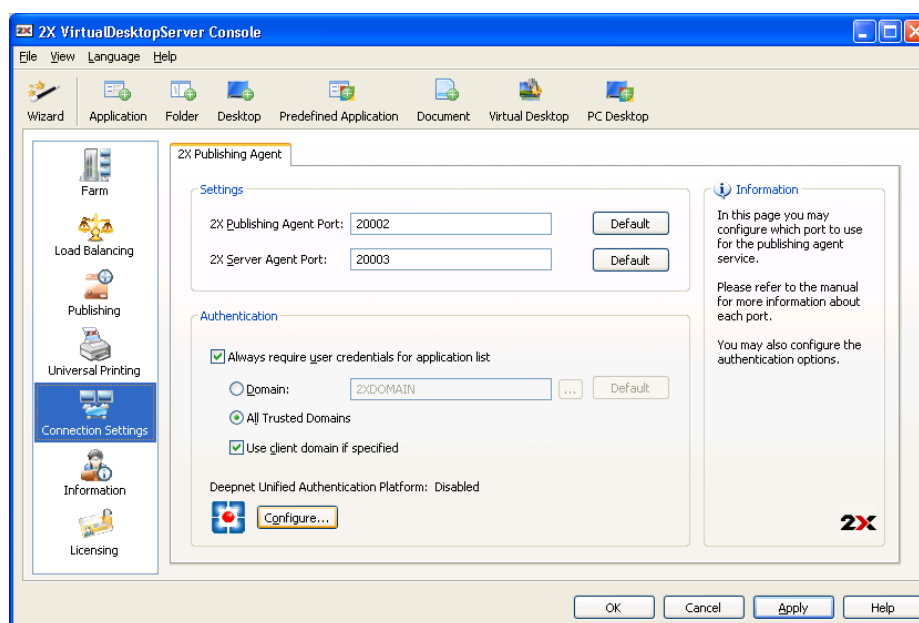


Figure 6: Connection Settings in 2X Console

Open 2X Console and click on the 'Connection Settings' section and browse the 'Publishing Agent' tab. Click on the 'Configure' button to open your Deepnet settings.

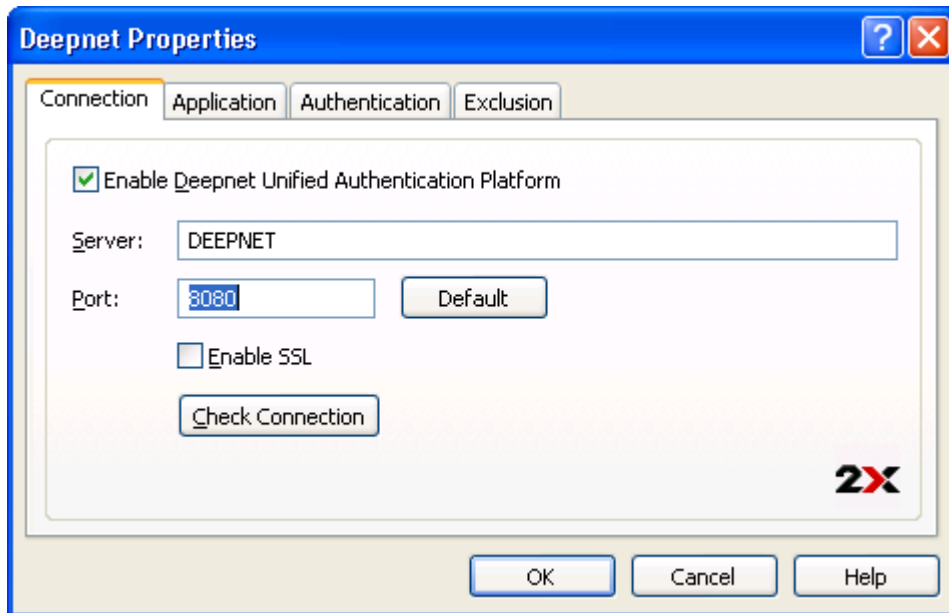


Figure 7 - Deepnet Unified Authentication Platform: Connection Properties

Connection

First check the 'Enable Deepnet Unified Authentication Platform'.

Enter the server name and port that you saved while setting up your Authentication Sever. Click on 'Check Connection' to test that you Authentication Server can be reached. You can choose to connect over SSL to your Deepnet server.

Application

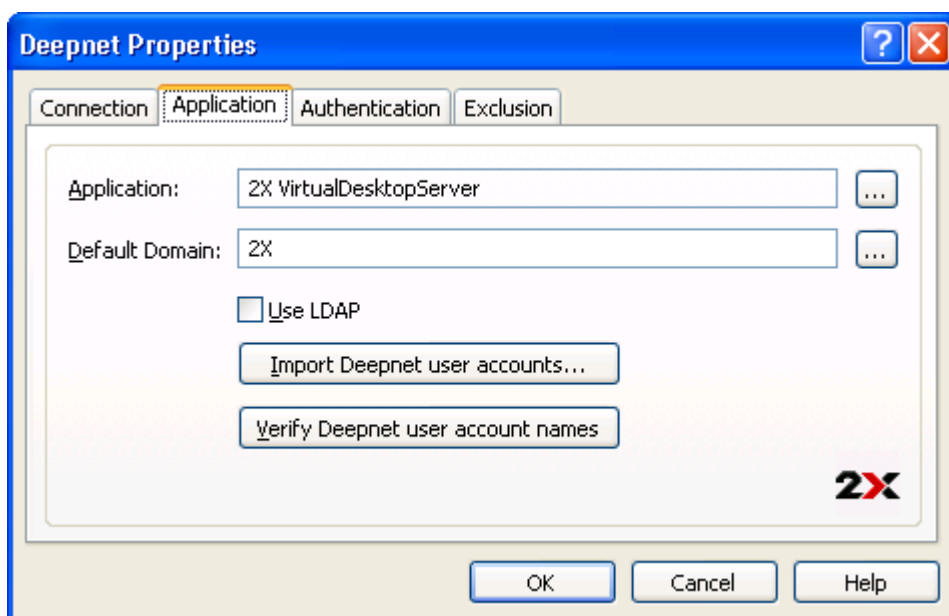


Figure 8 - Deepnet Unified Authentication Platform: Application Properties

Select the application profile that will use Deepnet to authenticate its users.

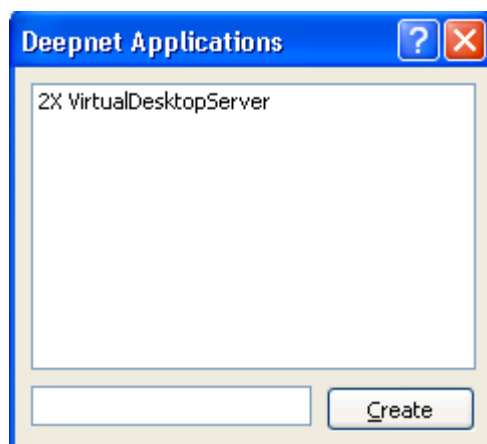


Figure 9 - Choose 2X VirtualDesktopServer

From the above dialog you can choose the application which used by 2X VirtualDesktopServer for authentication. You can also create an application which will be added on the Deepnet server.

The 'Default Domain' enables you to choose the default domain user for authentication and when users are added. Any Deepnet user accounts imported or verified will be done so using this default domain.

LDAP must be used when importing Deepnet user accounts and a group that contains other sub-groups.

'Import Deepnet user accounts...' automatically adds the specified users/groups into the Deepnet application.

'Verify Deepnet user account names' checks that all the users in the Deepnet application are in the following format: \\domain\username. Users added in the format of username@domain will be automatically changed to the appropriate format and users without a domain will have the default domain assigned to them.

Authentication

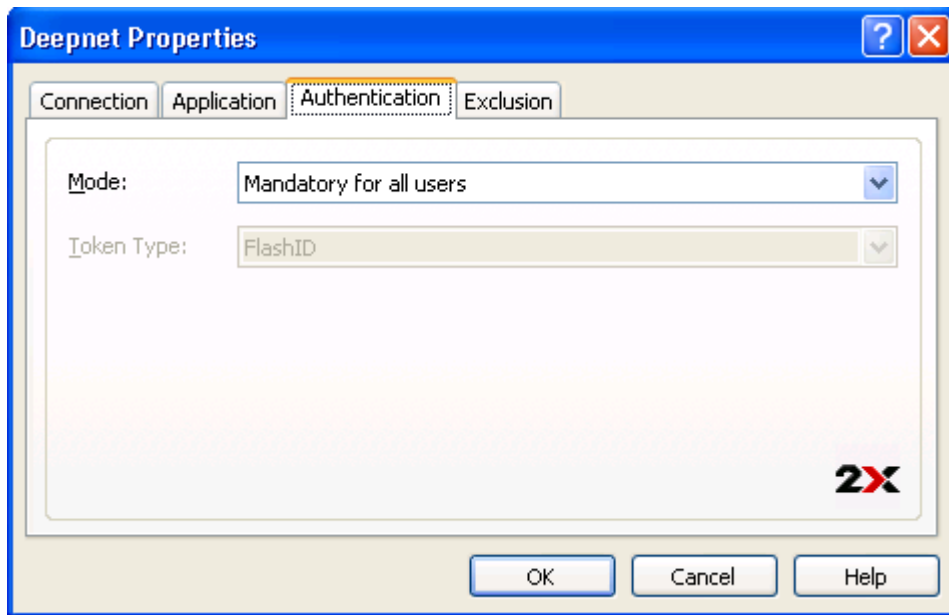


Figure 10 - Deepnet Unified Authentication Platform: Authentication Properties

Select how you want your users to be authenticated.

'Mandatory for all users' means that every user using the system must log in using two-factor authentication.

'Create token for Domain Authenticated Users' will allow 2X VirtualDesktopServer to automatically create software tokens for Domain Authenticated Users. Choose a token type from the drop down list. Note that this option only works with software tokens.

'Use only for users with a Deepnet account' will allow users that do not have a Deepnet account to use the system without have to login using two-factor authentication.

Exclusion

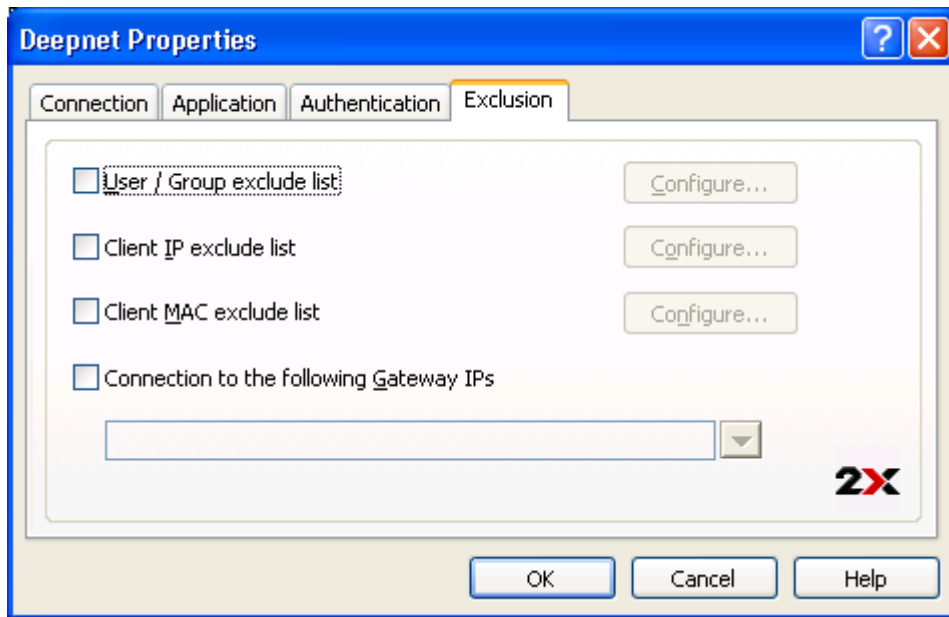


Figure 11 - Deepnet Unified Authentication Platform: Exclusion Properties

'User / Group exclude list' allows you to add users or groups within your active directory that will be excluded from using Deepnet Authentication.

'Client IP exclude list' allows you to add IP addresses or a range of IP addresses that will be excluded from using Deepnet Authentication.

'Client MAC exclude list' allows you to add a MAC addresses that will be excluded from using Deepnet Authentication.

'Connection to the following Gateway IPs' allows you to set a Gateway where users connected to the Gateway will be excluded from using Deepnet Authentication.

CREATING USER ACCOUNTS ON DEEPNET

When adding new user accounts on Deepnet it is important that the **domain name** is included with the 'Login Name' of the user therefore the entry should be in the following format: \\domain\username.

Users created automatically by 2X applications are already in that format but users imported from the Deepnet console must be corrected.

To correct the usernames, click on 'Verify Deepnet user account names' from the Deepnet Properties dialog.

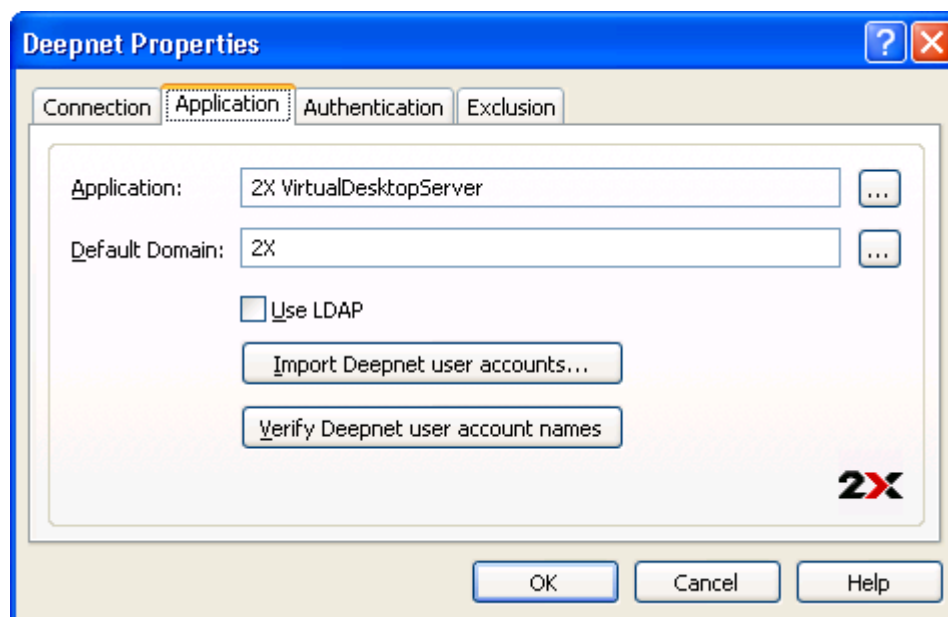


Figure 12: Set2XDeepnetUsers application

Note that users added in the format of username@domain will be automatically changed to the appropriate format (\\domain\username).

CONNECT TO A TERMINAL SERVER CONNECTION

Connect to a Terminal Server Connection

Once Deepnet has been enabled the users will have two-factor authentication. If using software tokens such as QuickID the administrator does not have to create a token for each user. 2X Publishing Agent will automatically create the token when the user tries to log in for the first time.

When a user tries to access a 2X Connection from 2X ApplicationServer Client, he/she is first prompted for the Windows username and password. If the credentials are accepted 2X Publishing Agent will communicate with the Deepnet server to create a unique token for that user.

The token then needs to be activated. Click on a button to send the activation code by e-mail or by SMS from the login window being shown by 2X ApplicationServer Client. A message will then be sent containing the token activation code.

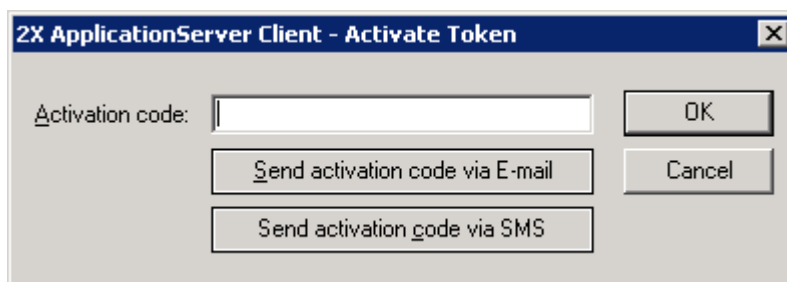


Figure 13: Obtain your activation code via SMS or E-Mail

If using MobileID or FlashID an email about where you can download the appropriate software will be sent to the user.

If using QuickID tokens, the application will ask for a One-Time Password which is sent by e-mail or SMS.

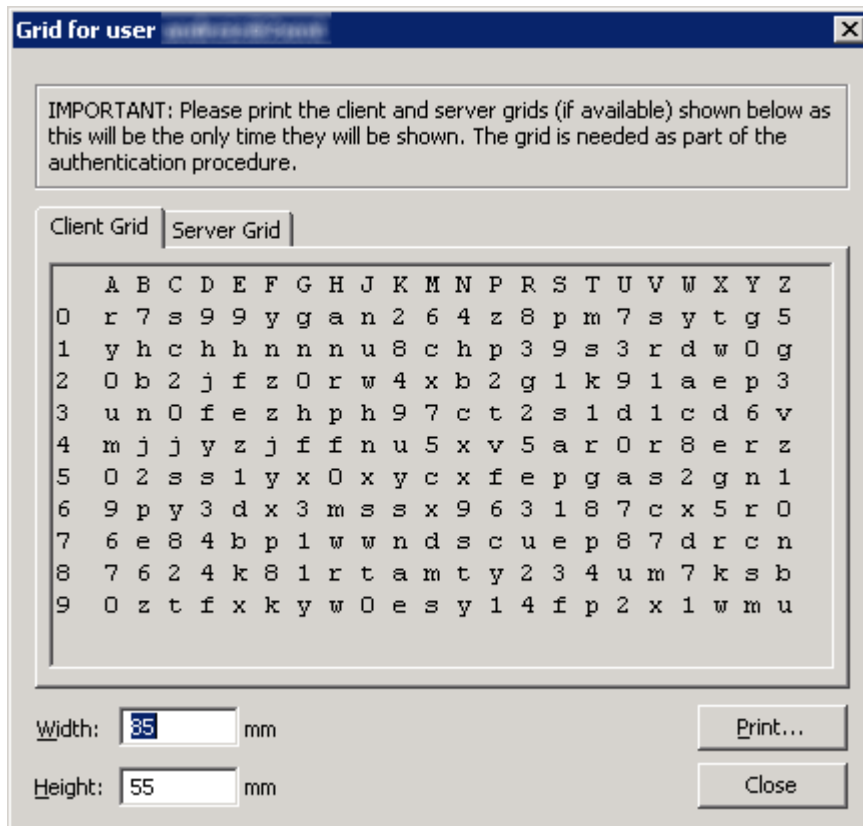


Figure 14: GridID matrix

If using a GridID, the user is given the opportunity to print the grid from the client itself. Note that this is only available the first time the user logs on.

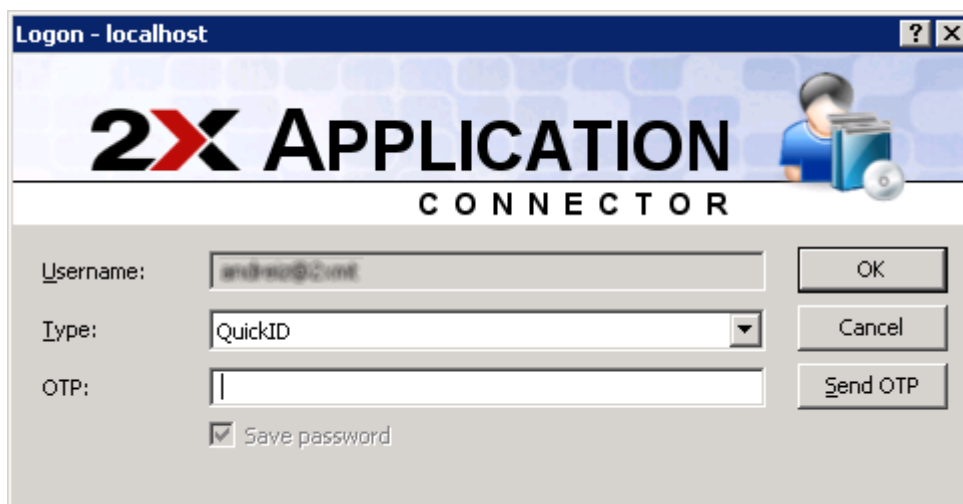


Figure 15: After receiving you One-Time Password input it in the OTP field

Enter the One-Time Password to log into the Terminal Server Connection.

2X ACCESS PORTAL

If Deepnet Unified Authentication is enabled, logging to 2X Access Portal also requires 2nd Level Authentication.

The screenshot shows the 2X Access Portal login page. At the top left is the 2X logo and the text "ACCESS PORTAL". At the top right are language selection links: [\[en\]](#) [\[de\]](#) [\[ru\]](#) [\[fr\]](#) [\[jp\]](#) [\[it\]](#) [\[es\]](#). Below this is a header "Welcome to the 2X Access Portal." and a "Please Login" form. The form contains a "Username:" field with the value "2xuser", a "Method:" dropdown menu set to "QuickID", and an "OTP:" field. Below the form are two buttons: "Send OTP" and "Log In". At the bottom of the page, it says "2X Client installed. Version: 7.0 (build 650)", "Powered by 2X.", and "Copyright © 2005-2009 2X Software Ltd."

Figure 16 – 2X Access Portal Using Deepnet