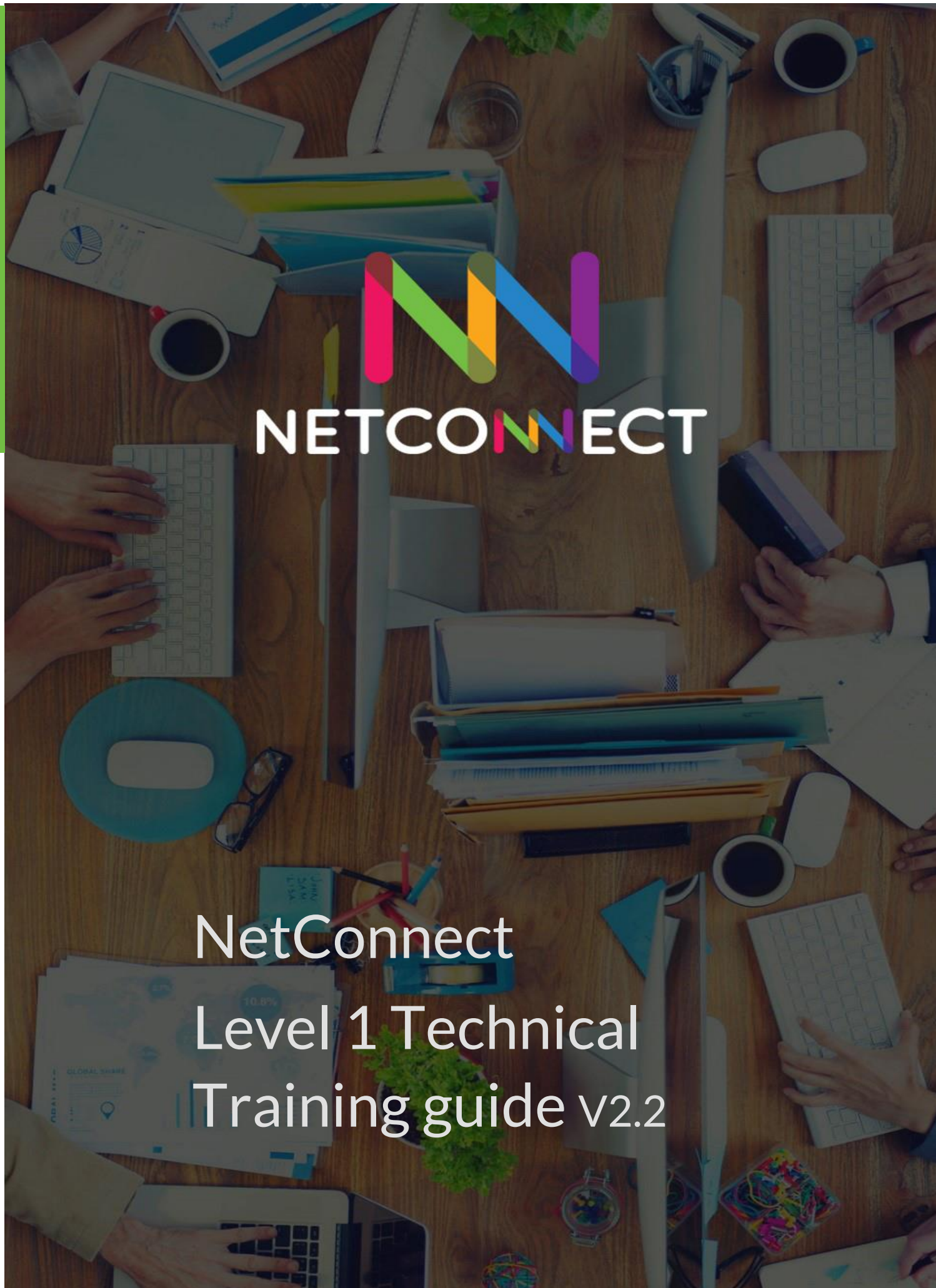


NETCONNECT

NetConnect Level 1 Technical Training guide V2.2

Contents

Chapter 1 – Overview

Training Objectives and Audience

This training is designed for system administrators looking at learning the basics skills required to install and maintain a NetConnect environment. NetConnect is simple to use and deploy, however a minimum level of technical understanding is expected. If you are not familiar with IP addressing, active directory or SSL certificates for example, this training may not be the most appropriate for you.

At the end of this training, administrators will be able to:

- Access the latest downloadable NetConnect environment
- Understand the requirements for a typical NetConnect deployment
- Install NetConnect in a live environment
- Install a license and a certificate
- Configure NetConnect to:
    - Enable access to Microsoft remote desktop
    - Configure authentication via local or active directory integration
    - Configure multiple authentication steps to enable MFA
    - Manage user access to various applications available in NetConnect
- Troubleshoot the basic issues

This guide is based on an installation of NetConnect 8.4.0.15.

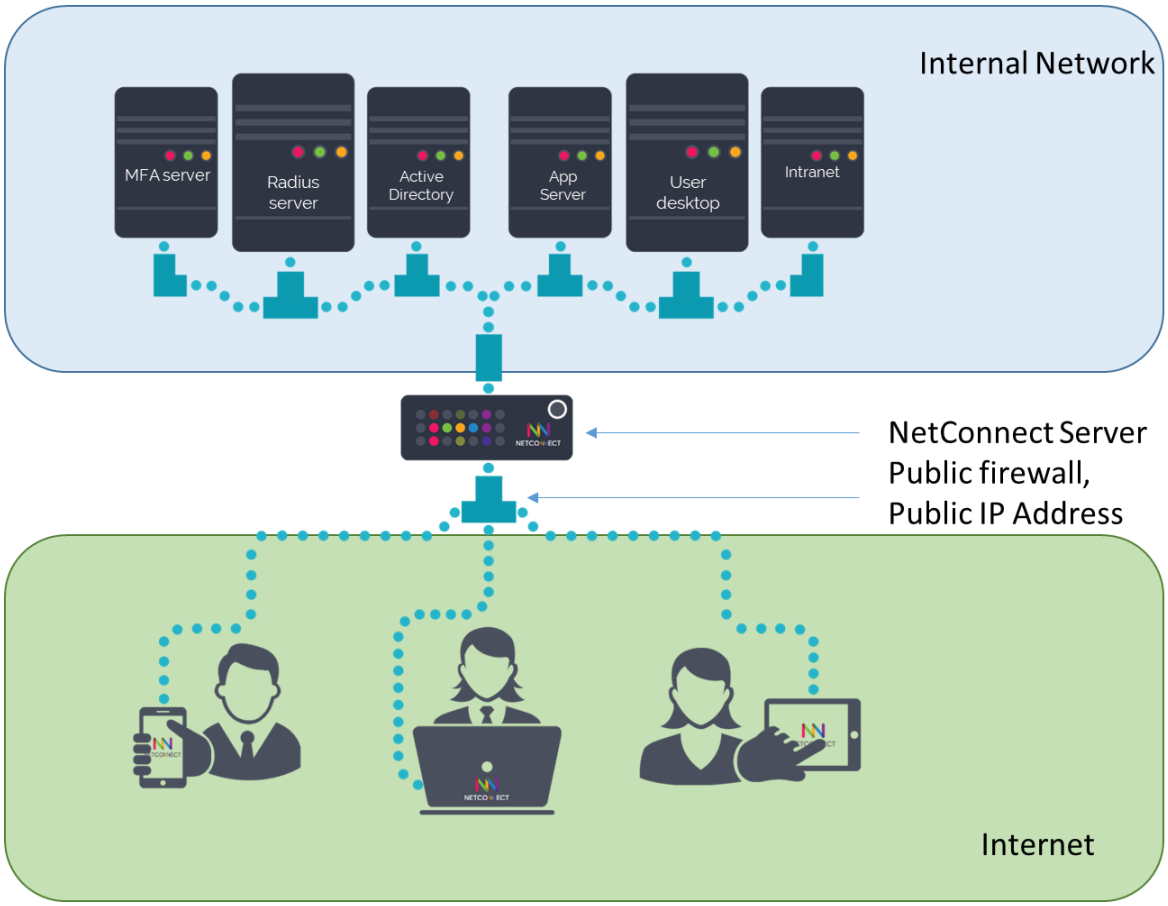
Understanding a typical deployment

NetConnect is a gateway situated at the edge of the customers network. This network can be located on premise or in the cloud. NetConnect will usually be installed as close as possible to the destination environment – i.e. if the customers network is located in the cloud, NetConnect will be best deployed in that cloud environment. NetConnect runs on top of a CentOS 6.8 installation, which comes ready-installed on our pre-prepared virtual and cloud installation packages. NetConnect allows for up to two network interfaces.

A typical deployment of NetConnect will follow standard steps:

- Download and install the latest software – pre-installed images are available for most common hypervisors and cloud environments. A manual installation procedure is also available upon request to the customer support team if required.
- Local network integration: Set up local IP address, DNS, etc.
- Installing licenses and certificates
- Configure user authentication – local or LDAP, multi-factor authentication, etc.
- Configure and test applications

This guide will generally follow the same standard steps, with a particular focus on hands-on activities.



Training Preparation – Requirements

In order to complete this training and perform the hands on activities, it is recommended you have the below. Note, this training is based on Hyper-V however other hypervisors will work similarly.

- Access to a virtualisation environment with enough available resources to meet the minimum specs.
    - 2GB RAM, 1CPU, 40GB HDD
- Access to the Internet
- Access to a windows Active directory environment, ideally with administrator access
- Access to windows remote desktop servers or a Windows PC, with administrator access

Optional:

If you are looking at enabling external access to your NetConnect deployment, you will also require access to a public IP Address and the firewall separating your NetConnect server and the Internet.

You can also use your DNS server to create your own access to NetConnect, however we can provide you with a temporary DNS entry with certificates if need be, to avoid the necessity to make changes to your production servers.

www.trialnetconnect.com

The website https://www.trialnetconnect.com can provide you with a temporary license, a temporary URL and a temporary certificate to use on your server to allow you to fully complete the training and have a fully functional NetConnect environment.

Chapter 2 – Installation and Network integration

Overview

- Download the virtual image
- Create a virtual machine
- Connect to the console
- Network configuration
- Admin portal connection
- Admin portal overview
- Change Admin passwords

Requirements

- A Hyper-V server
- Internet connection

Step by step guide

Objective	*Step by step*
Download the NetConnect virtual image	- Open a browser - Connect to https://northbridgesecure.com/software - Select Hyper-V - Download the image file.
Install the VHD on Hyper-V	- Open the Hyper-V console - Click New, Virtual Machine - Change machine name - Keep Generation 1 - Startup memory 2048 Mb - Network – use the appropriate virtual switch – this will be dependent on your environment. - "Use an existing Virtual Hard Disk". Select the file recently downloaded. - Click Finish.
Set a static, internal IP Address	- Right Click on the machine and click Connect. - Click on "Start" - Observe the server booting up to the NetConnect welcome page. - Connect as netconfig, and set up the network parameters. - Watch the server reboot, and see the new prompt.
Access your NetConnect Instance from a browser	- Open a browser and enter the IP Address you used for your server. - Accept the certificate error (no certificate is installed yet) - Accept the EULA

Admin Portal overview	- Connect as admin/adminv8 - Click on “Admin” - Familiarize yourself with the layout and the menus on the left
Change the default admin passwords	- Navigate to “Manage Access” -> change Password - Change the default password to a secure password. - Log out and also change the passwords for the following admin accounts: - radmin / r@dmin801 - maint / m@intain801

Chapter 3 – Licensing and Certificates

Overview

- Requesting a license
- Installing a license
- External network configuration overview
- Installing a certificate

Requirements

- Installed NetConnect server
- Access to NetConnect admin console
- A public IP address with port 443 available
- Access to change firewall settings
- Access to SSL certificate provider (optional)
- Access to add an A record to your DNS (optional)

Note: The Northbridge Secure mobile apps (both iOS and Android) depend on having a valid SSL certificate installed on your NetConnect instance..

Step by step

Objective	*Step by step*
Requesting a license	- Access your MAC Address by navigating to System Configuration -> Network -> General - Copy the MAC Address for Eth0 Interface - Request a license by sending this MAC to customersupport@northbridgesecure.com, or generate a trial license on https://www.trialnetconnect.com
Installing a license	- Navigate to System Configuration -> Licensing. - Paste the license key into the text box. - Click Submit - The license should show immediately, with all indicators showing OK.
External network configuration overview	- For your NetConnect server to be accessible from the Internet, some configuration is required on your local network: port 443 (https) must be forwarded from your external firewall to port 443 on your NetConnect server. - Note: port 443 is the only required port. You can also forward port 80 (http), knowing that this will only trigger a redirection to port 443 and is only to simply end user interaction.
Installing a trial certificate	- Navigate to System configuration -> General -> SSL -> Load Existing Cert - Copy the Private Key and the Certificate in the appropriate fields - Click submit - Click Set New Keys - Click Restart.

	- Close tabs, log back in.
Create a CSR for a production URL	- Navigate to System Configuration -> General -> SSL -> Certs From CA -> Request New Certificate - Fill in the form - Click “Generate New Certificate” - Copy the certificate and send it Note - The Certificate must correspond to the DNS A record in your DNS server. Note – NetConnect does not accept wild card certificates
Install a new SSL certificate from a provider	- Navigate to System configuration -> General -> SSL -> Certs From CA -> Upload Cert From CA - Copy the certificate into the box - Click submit - Click Set New Keys - Click Restart. - Close tabs, log back in.

Chapter 4 – Creating your first application

Overview

- Preparing the remote server for access
- Create a new application
- Allocate application to a user
- Review user experience
- Advanced features – printing, HyperDrive, copy/paste

Requirements

- Installed NetConnect server
- Licenced NetConnect server
- Access to the NetConnect admin console
- A Windows server or PC to establish a connection to

Step by step

Objective	*Step by step*
Preparing remote server for access	- Ensure NLA is turned off: - Open file explorer, right click "This PC", click properties - Click Remote Settings - Ensure "Allow remote connections to this computer" is on, and "Allow connections only from computers running Remote Desktop with Network Layer authentication" is unticked to enable access from non-domain users such as NetConnect local users.
Create a new application	- Navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select "Remote Application" for Application protocol - Enter the IP address in "Full Address" field - Switch "NLA Authentication" to off. - Click "Modify"
Allocate application to a user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Click on Local\admin, click on '<<' to allocate the application
Review user experience	- Sign out and log back in - Confirm the application is showing on the webtop. - Click on the application, and see the application open in a new tab - Familiarise yourself with the layout and the menu with arrow at the top of the screen.
Advanced features – printing,	- Navigate to Applications -> Configuration - Select your application, click on "General Properties"

HyperDrive, copy/paste	- Switch the following options to "on": Redirect Clipboard, Redirect Printers, Virtual Drive Upload. - Click Modify - Sign out and back in.
Advanced features – printing	- In a remote desktop session, try and print a document. - Allow pop up, print again. Observe the new tab opening up
Advanced features –HyperDrive	- Drag a file onto the session - The file is copied to the remote session on the N:\ drive and can be copied to other folders in the server
Advanced features –copy/paste	- Try copy/pasting text to and from the session - Note only plain text is supported. - Different browsers react differently, refer to our FAQ accessible from the top menu for more information.
Mobile Apps	- Download Northbridge NetConnect from either the App Store or Play Store. - Configure a Profile for your environment, using your Admin account. - Log in and launch you application. - Test either stand alone or with external display, mouse and keyboard.

Chapter 5 – Authentication basics

Overview

- Understanding V-Realms and authentication stages
- Create a local user data store
- Create a local user
- Create a V-Realm
- Create a local group
- Allocate an application to a user, a local group and a V-Realm
- Tips and tricks

Requirements

- Installed NetConnect server
- Licensed NetConnect server
- Access to the NetConnect admin portal
- An application configured on NetConnect

Step by step

Objective	*Step by step*
Understanding V-Realms and authentication stages	V-Realms are chained sets of authentication mechanisms used to confirm a users identity. A V-Realm can be as simple as username+password, or can request additional information such as one time passwords or MFA passwords before allowing a user into NetConnect
Create a local user datastore	- Navigate to Authentication Settings -> Datastores -> Internal Auth. Stores - Click “Create new Store” - Give the store a name, click “Create store”. - Click “Back to Stores list”
Create a local user	- Select your store, click “Get User List”, then “Add User” - Create a User.
Create a V-Realm	- Navigate to Authentication Settings -> V-Realm Management - Click Add-V-Realm - Name the V-Realm, Submit - Select Internal for Stage Type, Submit - Select your Authentication Store in the drop down box. Leave all other fields as they are. Click submit. - Open a different browser, open NetConnect. - Confirm the V-Realm is available, and the user can log in with this V-Realm.
Create a local group	- Navigate to Groups -> Local - Click “Add new Group” - Name the Group, submit

	- Allocate users to the Group - Allocate applications to the Group
Allocate an application to a user, a local group and a V-Realm	- Navigate to Applications -> Configuration - Allocate applications by using either “Authorized users”, “Authorized Groups”, or “Authorized V-Realm”.
Tips and Tricks: Rearrange V-Realm List	- Navigate to Authentication Settings -> V-Realm Management. - You can rearrange the order of the V-Realms by using the arrows below the V-Realm list -
Tips and Tricks: Direct Realm Access	- Give direct access to your users by adding the V-realm name at the end of your URL: - https://your_netconnect/realm/VrealmName -
Tips and Tricks: Hide Realm List	- Navigate the Authentication Settings -> Global V-Realm Properties -> V-Realm Pull-down Menu. - You can change the V-Realm drop down box to a standard text box to enhance security.
Tips and Tricks: Auto-Start Apps, Idle Timeout	- Navigate to Manage Access -> V-Realms - Select the Realm, Click Edit Realms Properties. - Add Startup apps to your Realm (for automatic launch upon web login), or configure an idle timer to disconnect users after a certain amount of inactive time.
Tips and Tricks: Assign Admin Access	- Navigate to Manage Access -> V-Realms - Select the Realm, click Get User list - Select a user, click General Properties - Change role to Radmin and click Assign - Navigate to Service -> Admin and move the user to the “Members” column using the arrows to complete the process.

Chapter 6 – Advanced authentication

Overview

- Bind NetConnect with an Active Directory instance
- Assign an application to an AD user
- Configure Single Sign on (SSO)
- Chain multiple authentication stages
- Configure Radius Authentication stage

Requirements

- Installed NetConnect server
- Licenced NetConnect server
- Access to the NetConnect admin portal
- Access to an Active Directory instance, reachable via NetConnect
- An AD account to bind with NetConnect
- A test account within the Active Directory

Step by step

Objective	*Step by step*

Bind NetConnect with an Active Directory instance	- Navigate to Authentication Settings -> V-Realm Management
	- Add V-Realm
	- Name the V-Realm
	- Select Stage Type LDAP
	- Fill in the following fields:
	  ○ Domain
	  ○ Host
	  ○ Port (389)
	  ○ Bind DN (found in your AD)
	  ○ Bind Password
	  ○ Base DN (end of the Bind DN)
	  ○ Login Attribute: sAMAcountName (Note – case sensitive)
	  ○ Group Member Attribute: member
	  ○ Group Base DN (same as Base DN)
	- Slick Submit
	- Test logging in as an AD Account

Assign an application to an AD user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Click on the appropriate 'Realm'\'User', click on '<<' to allocate the application
Configure Single Sign on (SSO)	- Navigate to Authentication Settings -> V-Realm Management - Select your V-Realm, click "Edit V-Realm's stages" - Click "Edit stage" - Enter a name for the authentication scope - Navigate to Applications -> configuration - Select your application, click Password Forward

	- Enter the same authentication scope. - Switch domain name forwarding to On. - Test connecting and opening a session with an AD user.
Configure Radius Authentication stage	Note - Any MFA solution which can be configured by Radius authentication can be incorporated into NetConnect. - Navigate to Authentication Settings -> V-Realm Management - Select your V-Realm, click “Edit V-Realm’s stages” - Click “Add stage” - Set type as Radius, submit - For demo purposes, use our publicly available demo Radius server: - Radius Server IP: 52.189.197.234 - Radius port 1812 - Radius secret: NetConnect - RADIUS Timeout: 60 - Click submit Note – This is not a production server and should only be used for training purposes. - Connect as an active directory user - The system is now asking for a second password – the password for our test radius server is demo

Chapter 7 – General Administration tasks

Overview

- Backup your server
- Restore a config backup
- Apply software update
- Reporting and Monitoring
- Shutdown and Restart

Requirements

- Installed NetConnect server
- Licenced NetConnect server
- Access to the NetConnect admin portal

Step by step

Objective	*Step by step*
Backup your server	- Navigate to System Configuration -> General -> Backup / Restore - Click Backup - Down the backup file Note - Backups can be scheduled to run on a daily, weekly or monthly basis.
Restore a config backup	- Navigate to System Configuration -> General -> Backup / Restore - Click Choose file, select the file. - Click Restore. - Log off and back on.
Apply software update	- Get the software update file from the Northbridge secure website. - Navigate to System Configuration -> Software upgrade. - Upload the config file and wait for the upgrade to complete
Reporting and Monitoring	- Navigate to Reporting and familiarize yourself with the menus - Navigate to monitoring and familiarize yourself with the menus
Shutdown and Restart	- Navigate to System Configuration -> Shutdown - Click on Shutdown or Reboot.

Chapter 8 – Applications overview

Overview

- MyDesktop
- SSH and Telnet Access
- RDP via VNC
- RDP via Port Forwarder
- Web via Reverse Proxy
- SSL VPN Tunnel

Requirements

- Installed NetConnect server
- Licenced NetConnect server
- Access to the NetConnect admin portal

Step by step

MyDesktop

Objective	*Step by step*
Prerequisite	- Requires an IP address/Hostname of a PC you wish to connect to, and access to your Active Directory
Update NetConnect with AD attribute used to identify workstation address	- Navigate to Authentication Settings -> V-Realm Management - Select Training Realm, click on Edit V-Realm Stages, and then Edit Stage. - Enter 'facsimileTelephoneNumber' in the Workstation Address Attribute field. - Click Submit
Create a new application	- Navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select "Remote Application" for Application protocol - Set Remote Application Type as 'MyDesktop' - Complete the Domain field - Click "Modify"
Configure SSO	- Navigate to Applications -> Configuration - Select your application, click Password Forward - Enter the same authentication scope as configured on your LDAP authentication stage. - Switch domain name forwarding to On.
Configure your AD User with destination PC hostname	- Log on to Active Directory server - Open Active Directory - Navigate to your training user - Right click and select Properties - Open the Telephone tab

	- Ensure the fax field is populated with your destination PC IP Address or Hostname
Assign the application to your training user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Select the appropriate 'Realm'\'User', click on '<<' to allocate the application
Test application	- Log in as the training user, confirm MyDesktop app is present. - Click on the app. You will be taken to the PC configured on the training users AD.

SSH & TelNet

Objective	*Step by step*
Prerequisite	- Requires a device which can be connected to via SSH or Telnet
Create a new application	- Navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select "Remote Application" for Application protocol - Enter the IP address of the destination device in the "Full Address" field - Select Application Protocol as "SSH" - Click "Modify"
Assign the application to your training user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Select the appropriate 'Realm'\'User', click on '<<' to allocate the application
Test application	- Log in to your training user account, confirm application is present - Click on the app to launch your SSH session

RDP via VNC

Objective	*Step by step*
Download VNC	- Navigate to the PC you wish access via VNC - Navigate to the destination PC - Download and install TightVNC (https://www.tightvnc.com/download.php)

Install VNC	- Run the VNC installation program - Select Custom Install - Disable VNC Viewer - Ensure all Additional Task options are ticked. - Configure a Password, this is used when connecting to the device. For single sign, this must be the same as the password to the destination PC. - Complete the installation wizard
Configure VNC	- Once installed, right click on the VNC icon in the taskbar and select Configuration. - On the Server tab, uncheck the Serve Java Viewer to Web Client tickbox - Record the port number, this will need to match the port configured on the NetConnect application later. - On the Access Control tab, add the IP address of the NetConnect server and set the action to “Allow”.
Create a VNC Application on NetConnect	- On your NetConnect instance, navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select “Remote Application” for Application protocol - Enter the IP address of the destination PC in “Full Address” field - Select Application Protocol as “VNC” - Ensure the Server Port number matches the port number configured on your destination PCs VNC configuration. - Click “Modify”
Assign the application to your training user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Select the appropriate ‘Realm’\’User’, click on ‘<<’ to allocate the application
Test application	- Log in to your training user account, confirm application is present - Click on the app to launch your VNC session - You will be prompted to enter the password configured on the destination PCs VNC configuration. - Once you click connect, you will have access to your destination PC via VNC.

RDP via Port Forwarder

Objective	*Step by step*
Install Java on the PC you wish to access the application from	- From the location you wish to connect from, navigate to https://java.com/en/download/ and download and install the latest version of Java.
Create a new PF application	- On your NetConnect instance, navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select "Remote Application" for Application protocol - Enter the IP address of the destination PC/server in "Full Address" field - Switch the HTML5 Client to "Off" - Complete the Domain field - Click "Modify"
Configure SSO	- Navigate to Applications -> Configuration - Select your application, click Password Forward - Enter the same authentication scope as configured on your LDAP authentication stage. - Switch domain name forwarding to On.
Assign the application to your training user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Select the appropriate 'Realm'\'User', click on '<<' to allocate the application
Test Application	- Open Internet Explorer - Navigate to your NetConnect instance and log in as your training user. - Click on your new application to launch. - Click through the prompts to complete the launch. Note, this may take a few minutes on the first connection.

Web via Reverse Proxy

Objective	*Step by step*
Create a new WRP application	- On your NetConnect instance, navigate to Applications -> Configuration - Click Create New Application - Give the application a name, select "Web via Reverse Proxy" for Application protocol

	- Enter the full URL in the Application URL field. For the purpose of the training, use https://northbridgesecure.com/ if you do not have your own internal intranet site - Click "Modify"
Create a Policy Rule	- Select the app and click "Policy Rules" - Change the protocol to HTTPS - Enter the Host Address as "northbridgesecure.com". Note, "https://" is not required. - Enter the Port as 443 and click create.
Assign the application to your training user	- Navigate to Applications -> Configuration - Select the application, click Authorised Users - Select the appropriate 'Realm'\'User', click on '<<' to allocate the application
Test application	- Log in to your training user account, confirm application is present - Click on the app to launch your WRP application

SSL VPN Tunnel

Objective	*Step by step*
Configure the Tunnel Settings on NetConnect	- On your NetConnect instance, navigate to Services -> Tunnel -> General Properties - Confirm the IP Address of the Tunnel Interface is valid for your network and does not clash with any other device. - Confirm the Client IP Address Range is a valid range for your network.
Download and Install the SSL Tunnel Client	- Navigate to Services->Downloadable Components and select the Windows Standalone Tunnel Client. - Once downloaded, install on the required PC and run the client from C:\Program Files\AEP\SSLTunnel.
Run the Client and Test Connection	- Once the client is running, enter the URL of your NetConnect instance in the Remote Host field and click Connect - Enter the relevant Realm, Username and Password for your training user and click connect to establish the SSL tunnel connection.