



NetConnect 8.4.0
Configuration Guide v1.7

Version Information

Date	Version	Author	Notes
31/03/2017	V1.0	James Newell	Initial Release
05/06/2017	V1.2	James Newell	Amendments to Hyper-V installation process
25/09/2017	V1.4	Janak Patel	Adjustments made for 8.4.0
27/09/2017	V1.5	James Newell	Copy + Paste section added.
19/10/2017	V1.6	James Newell	VMWare install modification
7/11/2017	V1.7	James Newell	Updated 'unlisted applications' details.

Contents

Supported Versions.....	4
Chapter One. Installation.....	5
1.1 Virtual Installation.....	6
VMWare Installation.....	6
Hyper-V Installation.....	8
1.2 Cloud Installation.....	11
Azure.....	11
AWS.....	11
1.3 Physical Installation.....	13
Overview.....	13
Chapter Two. Authentication.....	15
2.1 Administrator Access.....	15
Understanding Administrator Accounts.....	15
2.2 V-Realms.....	21
V-Realms Overview.....	21
Creating a V-Realm.....	23
Creating an Authentication Stage within a V-Realm.....	24
Creating an LDAP Authentication Stage.....	24
Creating an SMB Authentication Stage.....	26
Internal Authentication.....	27
Two Factor Authentication.....	31
Managing V-Realms.....	33
Chapter Three. Application Configuration.....	35
3.1 HTML5 RDP Applications.....	35
Configuring a MyDesktop Application.....	38

3.2	Configuring an SSH or Telnet Application	40
3.3	Configuring a VNC Application	42
3.4	Advanced Application Configuration.	48
	Advanced Properties.....	48
	Copy & Paste (beta).	49
	Enabling HyperDrive.	50
	Setting Up Single Sign On (SSO) via Password Forwarding.....	51
	Printing.....	52
	Utilising Multiple Servers for a Single Application.....	54
	Application Management.	57
4.1	Production Readiness	60
	Assigning SSL Certificates.....	60
	Network Changes.....	64
	Changing an Administrator's Password	64
	Licensing.....	65
	Customisation	66
4.2	System Administration.....	68
	Configuring General Settings	68
	Reporting.....	71
	Backing up and Restoring NetConnect Configuration	73
	Upgrading NetConnect.	75
	Shutdown and Restart.	77

Introduction

The purpose of this document is to provide a single source of information for the core features of NetConnect Release 8. This document will cover the most common steps involved with configuring and deploying a NetConnect instance. This document is split into four main sections; **Installation**, **Authentication**, **Application Configuration** and **System Administration**.

Should you require assistance beyond this document, please contact:

customersupport@northbridgesecure.com.

Supported Versions

While this information may be relevant to other versions / environments, the ones stipulated here have been actively tested with positive results.

Product	Version
NetConnect	7.8.8.0 and above
Microsoft Windows Server	2008 R2 and above
Microsoft Windows Desktop	7 and above
Apple Mac (OS X)	OSX 10.9 and above
Apple iPhone, iPad & iPod Touch (iOS)	iOS 9 and above
Android	6.0 and above
Java	8.4x and above
Browsers (HTML5 applications)	Chrome, Firefox, Internet Explorer 11, Safari, Edge.
Browsers (Java Port Forwarder)	Internet Explorer 11, Safari.
Hardware	NSS5000, NSS50.

Chapter One. Installation.

For NetConnect Release 8.1 and above, our recommended approach is to utilise pre-configured images of NetConnect on a virtual platform, available from Northbridge Secure. Installation directly on to Centos 6.8 Minimal (a widely used distribution of Linux based on RHEL – Red Hat Enterprise Linux) is also possible. This chapter will cover the following:

- Virtual installation (VMWare).
- Virtual installation (Hyper-V).
- Cloud installation (AWS).
- Cloud installation (Azure).

Once you have completed the installation, you will be able to access your NetConnect instances web interface locally, via the default admin account; you will then be able to begin additional configuration, including:

- Integration with your Active Directory.
- Enabling Single Sign On.
- Apply an SSL Certificate to ensure secure, encrypted connections.
- Apply a licence to allow multiple users access.
- Publish multiple desktops or applications.
- Configure multi-factor authentication.
- Print to any locally configured printer.
- Configure groups and V-Realms for enhanced access management.
- Change default admin passwords.

All these topics and more are covered in subsequent chapters.

1.1 Virtual Installation

VMWare Installation.

Overview

This section is intended to act as a guide to installing NetConnect within a VMWare environment via a pre-configured .OVA file. Note, the NetConnect OVA file was created using vSphere 6, Virtual Machine 11.

Before you begin...

Prior to commencing your installation, you will require the following:

1. A capacity to install a virtual instance that meets the following minimum specs:
 - a. 2GB of RAM.
 - b. 1 CPU.
 - c. 40GB of hard disk space.
 - d. Internet access.
2. Logon credentials to the Partner Portal as supplied by Northbridge Secure.
3. A copy of the latest NetConnect OVA file. This is available on the Partner Portal.
4. 1 dedicated static internal/private IP address.
5. 1 dedicated static external/public IP address. Required to access your NetConnect externally.

Default Passwords

For reference, the default Admin credentials for console and web access are below:

Console:

Username: sadmin
Password: \$admin.v801

Web:

Username: admin
Password: adminv8

Installing the OVA

This document will pass over the standard OVA installation process and concentrate on the specific steps required for NetConnect. For steps on the standard OVA installation process, please refer to the publicly available [VMWare guides](#).

Note, at the **Desk Format** stage, we recommend selecting **Thick Provision Lazy Zeroed**

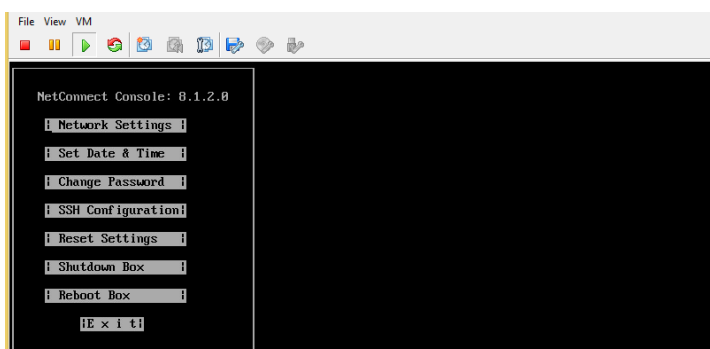
When selecting the network at the **Network Mapping** stage, ensure you select a network and subnet with access to the desktops/server/applications you wish to access via NetConnect

Once you have followed the deployment prompts, VMWare will provision your NetConnect VM based on the OVA file. Once completed, right-click on your new NetConnect VM, select "Open Console" logging in using the default console credentials (sadmin/\$admin.v801).

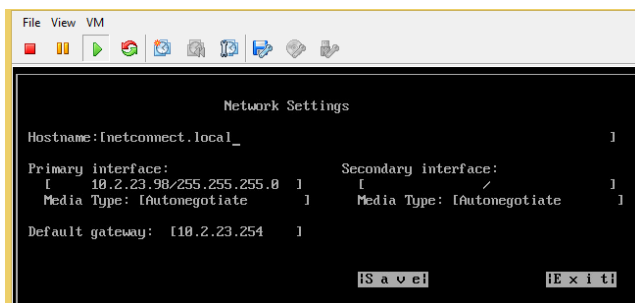
Configure Network Settings

Once you have connected via console, you will be required to configure your network settings in order to access NetConnect internally. When prompted for 'Terminal Type', enter the number 1 in your keyboard to select Linux. You will then be prompted to change the console password. **Ensure you record the new password in a secure location.** If the password is lost, there is no facility to recover.

Once the default password has been changed, next step is to assign the internal network details to the NetConnect server. When presented with the below screen, open the “Network Settings” page.



Once in the “Network Settings”, enter the **Hostname** and **Default Gateway** into the appropriate fields. Ensure the static Private IP address is entered under the **Primary Interface** field. Confirm all the information is correct, highlight **Save** and press the enter key. Below is an example of a completed Network Settings page using a single NIC configuration.



You will then be taken back to the main console menu screen. Go down to **Reboot Box** then press the enter key. After the server has rebooted, NetConnect will be accessible internally via the assigned static private IP using the default web credentials (admin / adminv8). If you are unable to reach NetConnect at this stage, you will need to delete the Network Adapter from you instance via the VMWare console and then add and configure a new Ethernet Adaptor.

Hyper-V Installation.

Overview

This section of the document is intended to act as a guide to trialling NetConnect within a Hyper-V environment. Installation will be via a prepared Hyper-V virtual machine which is available at the Northbridge Partner Portal. Note, the NetConnect virtual machine has been built using Hyper-V 6.3

Before you begin...

Prior to commencing your installation, you will require the following:

1. An active instance of Hyper-V, with configured network adaptors.
2. The capacity to create a virtual instance that meets the following minimum specs:
 - a. 2GB of RAM
 - b. 1 CPU
 - c. 40GB of hard disk space
 - d. Internet access.
3. Logon credentials to the Partner Portal as supplied by Northbridge Secure.
4. A copy of the latest NetConnect Hyper-V image. This is available on the Partner Portal.
5. 1 dedicated static internal/private IP address.
6. 1 dedicated static external/public IP address. Required to access your NetConnect externally.
7. Prior experience with Hyper-V.

Default Passwords

For reference, the default Admin credentials for console and web access are below:

Console:

Username: sadmin
Password: \$admin.v801

Web:

Username: admin
Password: adminv8

Installing the Hyper-V Instance

Installation of the NetConnect Hyper-V instance is a straight forward operation. This document will pass over the standard image installation process and concentrate on the specific steps required for NetConnect. For detail on the standard Hyper-V virtual machine installation process, please refer to the publicly available Hyper-V guides.

The current NetConnect Hyper-V image file can be downloaded from the Partner Portal. Note, this will come as a virtual hard disk which will be used to build the Virtual Machine.

From your Hyper-V Console, select **New > New Virtual Machine** and follow the below steps;

Before You Begin

Select '**Next**'.

Specify Name and Location

Define the name and storage location of the VM.

Specify Generation

Select '**Generation 1**'.

Assign Memory

Define the memory of the VM. The recommended size is 2GB or 2048MB.

Configure Networking

Select the relevant pre-configured Network adapter.

Connect Virtual Hard Disk

Select '**Use an Existing Virtual Hard Disk**', then use the browse option to select the NetConnect VHD downloaded from the Partner Portal.

Summary

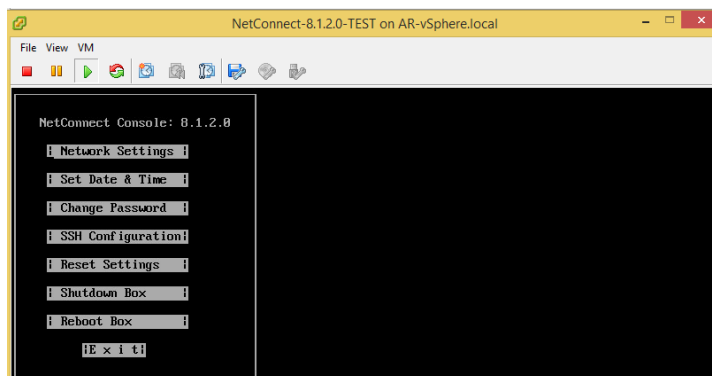
Review and finish.

Once you have followed the deployment prompts, Hyper-V will provision your NetConnect VM based on the pre-configured virtual image file. Once completed, right-click on your new NetConnect VM and select "start". This server will boot up and you will be presented with the console log in screen - log in using the default console credentials (sadmin/\$admin.v801).

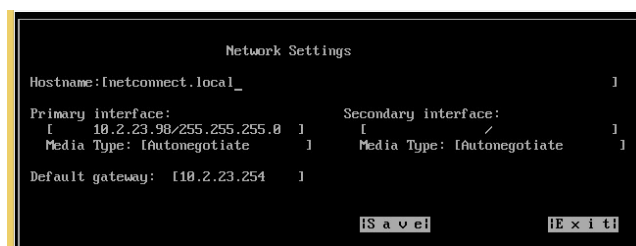
Configure Network Settings

Once you have connected via console, you will be required to configure your network settings in order to access NetConnect internally. When prompted for 'Terminal Type', enter the number **1** in your keyboard to select Linux. You will then be prompted to change the console password, you can opt to cancel this step. If you choose to change the password **ensure you record the new password in a secure location**. If the password is lost, there is no facility to recover.

Once the default password has been changed, next step is to assign the internal network details to the NetConnect server. When presented with the below screen, open the "Network Settings" page.



Once in the "Network Settings", enter the **Hostname** and **Default Gateway** into the appropriate fields. Ensure the static Private IP address is entered under the **Primary Interface** field. Confirm all the information is correct, highlight **Save** and press the enter key. Below is an example of a completed Network Settings page using a single NIC configuration.



You will then be taken back to the main console menu screen. Go down to **Reboot Box** then press the enter key. After the server has rebooted, NetConnect will be accessible internally via the assigned static private IP using the default web credentials (admin / adminv8).

1.2 Cloud Installation

Azure

Overview.

NetConnect can be installed directly from the Azure Marketplace. The NetConnect application on Microsoft Azure allows you to deploy simply and very quickly a full NetConnect server. The NetConnect deployment available on the Azure marketplace is pre-installed, allowing you to dive into configuration and be ready for your first connection within 15 minutes. Installation instructions can be found within [the NetConnect Azure MarketPlace page](#);

AWS

Overview

This document is intended to act as a guide to trialling NetConnect within AWS. In it, we will cover the key steps involved with installing a fresh instance of the latest NetConnect release and publishing a desktop. Installation will be via a prepared Amazon Machine Image (AMI), which is available via the AWS Community AMI portal. This document is intended for administrators looking to install NetConnect for evaluation purposes. By the end of this document, you will have published an AWS server desktop via NetConnect.

Once you have completed the installation steps detailed in this document, additional configuration can be performed in order to access additional features and expand functionality.

Before you begin...

Prior to commencing your installation, you will require the following – each of these points are detailed within this document and accompanying video:

1. An account with AWS.
2. An existing server within AWS that you wish to connect to via NetConnect.
3. Virtual Private Cloud configuration in place.

Default Passwords

For reference, the default Admin credentials for NetConnect are below:

Username: admin
Password: adminv8

Installing the AMI

Installation of the NetConnect AMI is a straightforward operation. This document will cover the specific steps required for NetConnect. For further information on AWS AMIs, please refer to the AWS website.

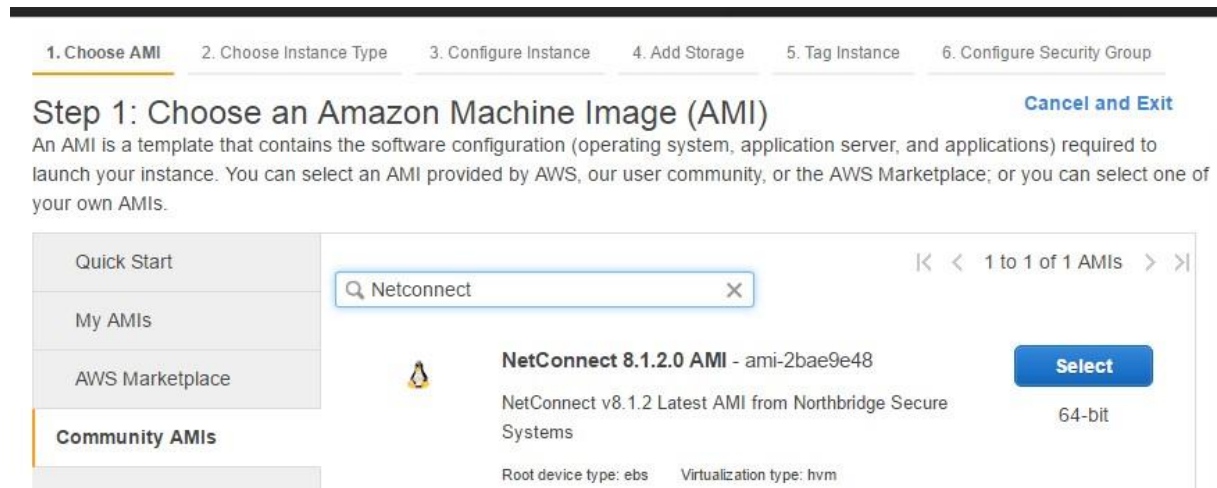
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>

Installation

Log in to your AWS account, navigate to 'EC2' and select 'Launch instance'. You will then be able to follow the installation via the standard AMI wizard.

Step 1: Chose an Amazon Machine Image (AMI)

Under the 'Community AMI' section, search for "NetConnect" and **select** this image:

*Step 2: Choose an Instance Type*

We recommend using the instance type **T2 Small**, as this meets the minimum specification of 1 CPU & 2GB RAM.

Step 3: Configure Instance Details

Ensure you select a network and subnet with access to the server(s) you wish to access via NetConnect. **Ensure** you enable **Auto-Assign Public IP**. All remaining settings are to be configured to your specific AWS requirements.

Step 4: Add Storage

The AMI storage is pre-configured with 40GB and does not require any further configuration.

Step 5: Tag Instance

Tag your instance as required, for example 'NetConnect Trial'.

Step 6: Configure Security Group

Create or assign a security group that allows **port 443 from any location**, as well any other environment specific requirements.

Step 7: Review Instance Launch

Review the settings and select **Launch**, you will then be presented with key pair options. While you will need to select/create a key pair and tick the acknowledgement in order to complete the process, NetConnect is configured with default credentials and as such key pairs will not be relevant.

After a short while your NetConnect server will be accessible from 'Instance' window. Once the standard automatic status checks have been completed NetConnect will be accessible via the Public IP.

Elastic IP

Note, by default the IP address assigned by AWS is dynamic and will change if the server is shutdown - it will remain after reboot. It is recommended that an elastic IP is assigned for any production environment instance as access will be via a URL which relies on a static IP configured via DNS.

1.3 Physical Installation

Overview

This section describes how to install NetConnect onto an NSS5000 or NSS50 appliance. With this approach, CentOS 6.8 will be applied to the appliance (a widely used distribution of Linux based Red Hat Enterprise Linux), with a NetConnect TGZ file installed on top of this OS.). This section assumes the reader is comfortable with Linux command line interface.

Before you begin...

Prior to commencing your installation, you will require the following – each of these points are detailed within this document and accompanying video:

1. An NSS5000 or NSS50. **Note, this instance must have internet access in order to download required RPMs.**
2. A copy of CentOS 6.8 minimal. This is available from the Partner Portal.
3. 1 static internal IP address.

Default Passwords

For reference, the default Admin credentials for NetConnect are below:

Username: admin
Password: adminv8

Installing CentOS

Installation of CentOS is a straight forward operation. If you need a step-by-step guide on how to install CentOS, please refer to the 'Install CentOS 6.8' section of below link. Note, you will use the root account at various points during the installation process, please be sure to record the credentials.

<http://lintut.com/how-to-install-centos-6-5-minimal/>

Installing NetConnect

Once your virtual instance is running CentOS 6.8 minimal, you're ready to install NetConnect.

CentOS Preparation

You need to download 'wget' tool which is a non-standard CentOS package for minimum install. To do this, run the following command from the shell prompt.

yum install wget -y

Then you will need to download the script that is required to perform the installation.

wget <https://s3-ap-southeast-2.amazonaws.com/nos-installer/runscript.sh>

When ready, run the following command to make the file executable.

chmod +x runscript.sh

Finally, run the below command to execute the script

./runscript.sh

Press any key to continue when prompted. CentOS will download and install the required files. After one to two minutes, you'll be presented with the network configuration interface.

- Enter 'Device Configuration'.
- Enter the network card you wish to configure.
- Arrow down and use the spacebar to toggle off 'Use DHCP'
- Enter the Static IP, subnet mask, default gateway, primary & secondary DNS server addresses into the relevant fields.
- Arrow down and use the spacebar to toggle off 'Controlled by NetworkManager' (spacebar).
- Select 'OK'.
- Select 'Save'.
- Select 'Save&Quit'.
- Press any key to continue.

At this point, the CentOS server will reboot and apply the changes.

Once your CentOS server has rebooted, connect via console to your CentOS image, log in as root and run the following commands:

```
cd /tmp
```

```
./netconnect.sh
```

Again, press any key to continue when prompted. This will run the NetConnect installation script, which will take between five to ten minutes. Once the installation has finished, you will be prompted to reboot; simply enter the command **reboot** and press enter.

Chapter Two. Authentication.

Once NetConnect is installed, there are several steps that can be taken to integrate with the internal infrastructure to allow access for specific users/accounts. From this stage, all configuration steps will be performed within the Administration page. Access to this area is restricted to Admin users. The Admin page can be reached by navigating to the assigned internal IP address configured during Chapter One, and logging on using the default Admin credentials:

Username: admin
Password: adminv8

This chapter will cover the following:

- An introduction to the Administrator accounts.
- An introduction to the Administrator page.
- V-Realms.
- Active Directory integration.
- SMB Authentication.
- Local User Authentication.
- Multi-Factor Authentication.

2.1 Administrator Access

Understanding Administrator Accounts

The following four default administrative accounts are provided:

- Auditor: The auditor account is the lowest privilege level. This is essentially a read-only account.
- Radmin (or reseller administrator): An account created for managing the service in the field.
- Maint: An account created for general maintenance and has the least number of privileges.
- Admin: This account has the highest privilege level.

Admin or Radmin provides the level of privileges necessary for configuration. It is recommended that all default passwords are changed prior to production roll out. All configuration instructions presented in this guide can be performed as admin or radmin. Exceptions are noted. The rights of each of the administrative accounts are listed in the following table:

Administrator Rights	Auditor	Radmin	Maint	Admin
Administer the product licences	No	Yes	No	Yes
Backup and restore configuration settings	No	Yes	No	Yes
Create, modify and delete application objects	No	Yes	Yes	Yes
Access and change network settings such as IP addresses	No	Yes	No	Yes
Activate and de-activate the internal firewall	No	Yes	No	Yes
Create, modify and delete users	No	Yes	Yes	Yes
Customise the login screen	No	Yes	No	Yes

Default Passwords

Default passwords can be found below:

admin

adminv8 (web)

sadmin – used for SSH and Console access.

\$admin.v801

radmin

r@dmn801

maint

m@intain801

Administrator Access Requirements

To access the Administrator Site, you will need the following:

- Supported web browsers:
 - Microsoft Internet Explorer 11
 - Microsoft Edge
 - Firefox version 4x.x
 - Chrome version 4x.x
 - Safari version for Mac OS X 10.9 and above
- A valid username and password, and the IP or URL of your NetConnect platform.

Logging in to the Administrator Site

To access the Administrator Site:

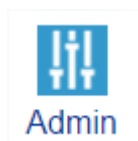
- Initiate a connection to the Internet and launch a Web browser.
- Enter the IP address you configured during the initial setup.

You will be presented with the log in page, as shown below.

The screenshot shows the NetConnect Web Portal login interface. At the top is the NetConnect logo, a stylized 'N' made of colorful vertical bars. Below the logo is the text 'NETCONNECT' and 'Welcome to the NetConnect Web Portal'. The login form contains three fields: 'User Name' with the value 'admin', 'Password' with masked characters, and 'V-Realm' with a dropdown menu showing 'Local'. A blue 'Log In' button is positioned below these fields. The footer of the page displays the NetConnect logo and the text 'Powered by NorthbridgeSecure'.

- For **User Name**, enter admin. This field is case-sensitive.
- For **Password**, enter adminv8. This field is case-sensitive.
 - The default password should be changed prior to production roll out.
- Make sure the **V-Realm** field is set to Local (or type Local in the V-Realm field if the V-Realm drop-down list is box is not displayed).
- Click **Log In**.

- The Licence agreement is displayed when you log in for the first time as admin. Accept the licence agreement by clicking Yes.
- Click the Admin icon to access the configuration pages referred to as the Administrator Site.



Home

Manage Access

Groups

Applications

Services

Reporting

Monitoring

Customization

System Configuration

Authentication Settings

Admin Home

Current, at a glance status that includes latest alerts, system status and number of active users.

Alerts Status:

Date	Level	Source	Event	Description

System Status: Fri Mar 31 12:24:12 EST 2017

Uptime	15 day 22 hours 20 minutes
Version	8.2.9.7
eth0 IP Address	
eth1 IP Address	0.0.0.0
Current load average	0.06
Memory Total/Used/Free	996.38M / 870.11M / 126.27M
Swap Total/Used/Free	2015.99M / 334.34M / 1681.66M
Last Backup	Fri Mar 17 13:45:26 2017

User Status:

	Current Active Users
Total Users	1
CMID	0
LDAP	0
local	1
SMB	0
Vasco2FA	0

The admin page can be used for the following:

- **Manage Access:** Assign applications, policies and other services to users and groups on a per V-Realm basis.
- **Groups:** Add and manage groups of users.
- **Applications:** Create pointers to the applications that you want users to be able to access.
- **Services:** Configure system-wide settings for each of the services.
- **Reporting:** Gather reports on usage statistics and the like.
- **Monitoring:** Gather and review product statistics some of which are based on time periods you specify.
- **Customisation:** Customise the login page with your company's name and logo.
- **System Configuration:** Configure network settings such as Ethernet and DNS settings, as well as install licences, manage digital certificates, backup system settings and restore system settings.
- **Authentication Settings:** Configure V-Realms and authentication states within V-Realms such as SMB, LDAP and RADIUS.

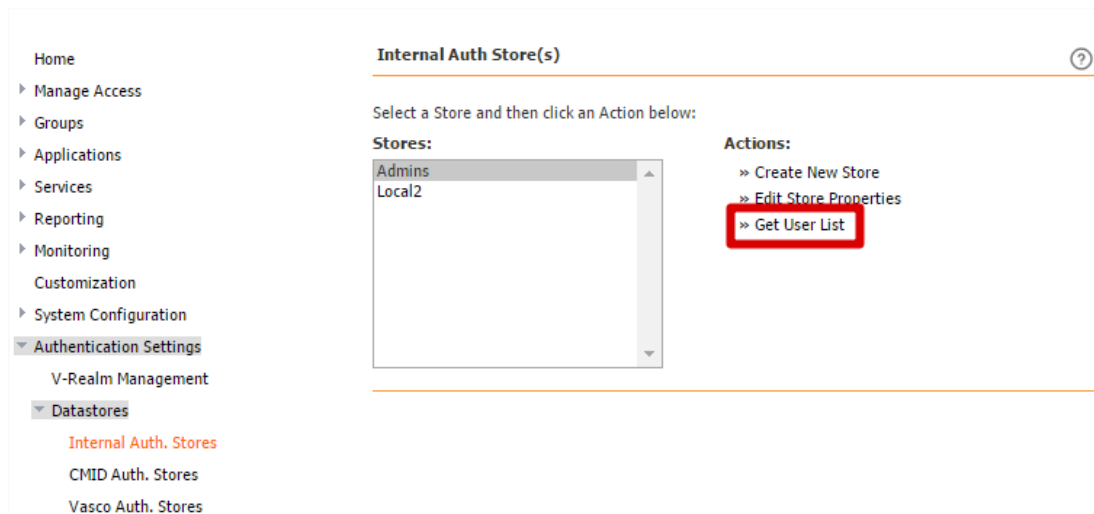
Changing an Administrator's Password

To change the password of your administrator account, follow the below:

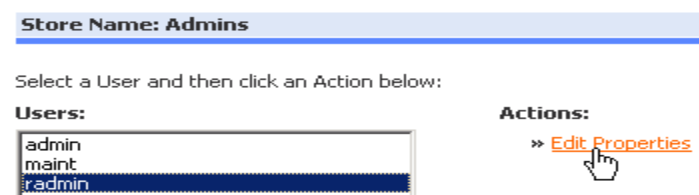
- From the Administrator Site, navigate to **Authentication Settings > Datastores > Internal Auth Stores**

WARNING: If you change the password for the admin account, be sure to document the new password and keep it in a safe location. If you forget the password you will not be able to access NetConnect and there is no other way to gain access.

- Select Admins and then click **Get User List** as shown.



- Select the admin account for which you want to change the password and then click **Edit Properties**.



The Password field is case sensitive. The password may have any alphanumeric character, or punctuation marks such as the following English punctuation marks: !"#%&'()*=-~^|\`@{[+,*:]<,>./_\. .

- Enter a new password in the **New Password** field and then type the identical password in the New Password Confirm field.
- Click **Update Password** to save the changes.

If you changed the password, log out and then log in again using the new password.

Configuring Role Based Administration

You can allow users to also assume the role of administrator by assigning administrator privileges to users and then granting them membership to the Admin Service. The various administrator roles that may be assigned to a user are Radmin, Maint and Auditor. Note that roles cannot be assigned or changed for the default administrator accounts (Admin, Radmin, Maint).

To assign administrator privileges to a user, do the following.

- From the Administrator Site, click **Manage Access**.
- Select the name of the V-Realm that you want to work with and click **Get The User List**. In the following example, test V-Realm is selected.

V-Realms

Select a V-Realm and then click an Action below:

V-Realms:

local
test realm

Actions:

- » [Get The User List](#)
- » [Edit Realm Properties](#)

- Select the name of the user to whom you want to add administrator privileges and then select **General Properties**. The properties page for that user appears:

V-Realm: realm 2

Select a User and then click an Action below:

Users:

user1

Actions:

- » [General Properties](#)
- » [Current Webtop](#)
- » [Applications](#)

- Locate the **Role Based Administration** section

Role Based Administration

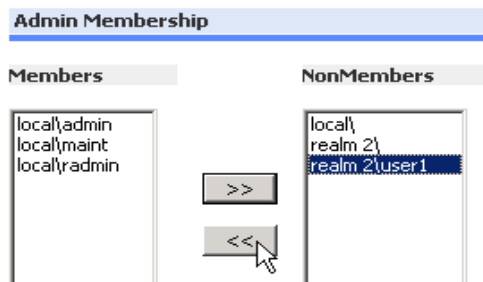
Select Role for User

Role: radmin Assign

None
radmin
maint
auditor

Idle Time

- Choose one of the following roles:
 - **None:** Choose None (the default setting) to prevent this user from having administrator privileges. When None is specified, the users only have user level privileges that have been allowed such as application access and the ability to change their own passwords.
 - **Radmin:** Choose Radmin to allow this user to also have radmin level administrator privileges.
 - **Maint:** Choose Maint to allow this user to also have Maint level administrator privileges.
 - **Auditor:** Choose Auditor to allow this user to also have an auditor role. Auditor provides read only access to the administrator site. Attempts to change settings result in error messages indicating that the user is not authorised.
- Click **Assign**. You will be prompted to confirm that you want to change the role for this user.
- Click **OK** to confirm.
- Navigate to **Services** menu, select Admin. The Membership page for the various administrator accounts appears.
- If the name of the user whose role you just changed is in the NonMembers column, select the user name and then click the right arrow to move it to the Members column as shown:



The user is now a member of the Admin service and, if administrator privileges were added, then those additional privileges are now in effect.

The next time the user logs in, the Admin icon will appear on the WebTop.

2.2 V-Realms

NetConnect can be configured to allow user authentication in a number of ways. Authentication is built around the concept of V-Realms, which allow for advanced authentication management.

V-Realms Overview.

The advanced V-Realms client identity engine simplifies the provisioning of authentication and entitlements, which can include employees, partners and affiliated authorised users (such as physicians affiliated with a hospital).

This section presents a conceptual overview of V-realms and their implementation. A user's association with a V-Realm determines the user's method of authentication, and also determines the authentication server(s) against which a user's credentials are validated.

Each V-Realm page can be customised with unique company names, logos and messages. Please refer to the 'Customisation' section of this guide for further details.

About the Local V-Realm

By default, there is a V-Realm named "local" that uses internal authentication and contains the following administrative accounts.

Admin: The admin account is the highest privilege level.

Radmin (or reseller administrator): An account with fewer privileges than admin.

Maint: An account created for general maintenance and has the least number of privileges.

Adding Authentication Stages to the Local V-Realm

For stronger administrator authentication, you can add more authentication stages such as Active Directory, RADIUS or SMB to the local V-Realm. Details on how to configure specific changes are covered in this chapter.

V-Realm Considerations

Several items to consider when configuring V-Realm are listed below.

- To log in, every user must belong to a V-Realm.
- A user can only exist in one V-Realm. Duplicate names in two V-Realms are treated as unique users.
- You can create a maximum of 1,000 authentication V-Realms.
- All members of the V-Realm inherit all applications assigned to that V-Realm.

Authentication Stages within V-Realms

Authentication stages are defined within a V-Realm and are used to indicate the type of authentication server that validates a user's login credentials. Each defined authentication stage has two components, an authentication section and a policy section. The authentication section is required for any given stage. However, the policy definition is optional. Configuring policy enables retrieval of group membership information about users from external authentication servers when they log in.

Types of Authentication Stages within a V-Realm

Below is a list of some of authentication stages that can exist within a V-Realm.

Authentication Stage	Description
LDAP	Authenticates the user against the user account maintained on an external LDAP server.
RADIUS	Authenticates the user against the user account maintained on the external RADIUS server.
SMB	Authenticates the user against the user account information maintained on an external Windows Domain Controller.
Internal	Authenticates the user against the NetConnect internal user account information. The user account information is cryptographically maintained in NetConnect itself. Internal user account information is hashed in a form where the original password cannot be recovered.

Multiple Stage Authentication Within a V-Realm

For added security, you can set up multiple authentication stages within the same V-Realm. When a user logs in to a V-Realm that has been set up with multiple authentication stages, successful authentication must occur at every stage within that V-Realm before access is allowed. This is an important consideration when creating different stages within a V-Realm.

NOTE: A maximum of 10 different authentication stages can exist within a V-Realm.

Logging in as Multiple Users

By default, V-Realms with multiple stages are configured so that users log in with the same username for every stage. The user is challenged for username and password for the first stage, and then prompted only for their password at each subsequent authentication stage (i.e., the username is carried forward from stage to stage). This default arrangement, when the user name is the same between stages, provides a level of user convenience.

Alternatively, V-Realms can be configured to force users to log in using different user names as well as passwords for every stage. In effect, this allows a user to log in under different user names for the same session. There are several advantages to this arrangement, including:

- Users can access distinct systems (i.e., a UNIX server, and Windows terminal server, etc.) where they hold different accounts within the same session.
- Increased security.
- Administrators can log in with different administrative privilege levels for various administration needs, such as system testing.

This feature is configured when you create additional authentication stages within a V-Realm. The Authentication Stage properties page has a check box labelled “**Use same username as previous stage**”, explained later in “Creating an Authentication Stage Within a V-Realm”.

Multiple Landing Pages

With Multiple Landing Pages, different log in pages can be presented from a single site. Each page or landing area is differentiated by V-Realm. The text and graphics of each V-Realm portal page can be customised.

Once you have created V-Realms, simply add the suffix `/realm/"vrealmname"` to the URL to access each landing page. No additional configuration is needed.

For instance, with a host name of “myproduct” and two V-Realms, realm1 and realm2, type “/realm” after NetConnect’s URL and then type the realm name of the landing page you want to access. For example, if you have two landing pages and the associated V-Realms are “realm1” and “realm2” you would enter the following URL:

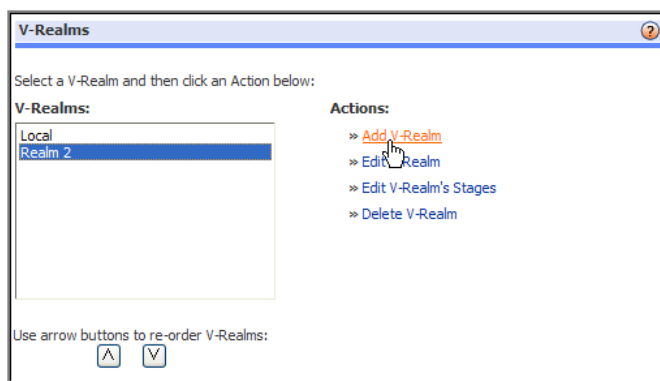
- www.myproduct.com/realm/realm1
- www.myproduct.com/realm/realm2

Only the following characters are allowed in a V-Realm URL: letters a through z; numbers 0 through 9, underscore “_”, dash “-” and dot “.” Letters used in a V-Realm can be upper or lower case but must be typed as lower case when entering the URL for a multiple landing page area. For example, if the V-Realm is configured as “MyRealm”, MYREALM” or “myrealm”, for all of these cases, the URL would be: https://virtual.northbridgesecure.com/realm/myrealm

Creating a V-Realm

This section describes the steps required to create a V-Realm.

- Log in as either the admin or radmin administrator account. Make sure the V-Realm name field is set to Local, or type Local in the Realm name field (when NetConnect is configured to hide the realm drop-down list box).
- From the Administrator Site, click **Authentication Settings**.
- Click **V-Realm Management**. The Authentication Settings page opens.
 - Note once you have created your V-Realm, you use the arrows buttons to change the order that V-Realms appear on the log on page.
- Click **Add Realm** as shown

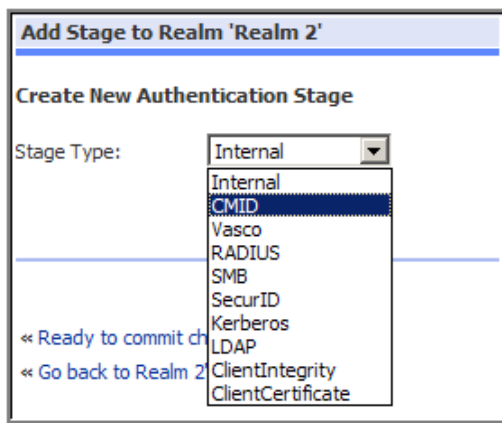


- Enter a name to identify the authentication V-Realm. Acceptable characters are letters (a through z), numbers (0 through 9), dash “-”, underscore “_” and period “.” The default V-Realm number is where # is the number of existing V-Realms plus one.

Create a New V-Realm

V-Realm Name:

- Click **Submit**. The following page appears.



To complete the creation of this V-Realm, you must define at least one authentication stage within it. See “Creating an Authentication Stage Within a V-Realm” within section 2.2 for further details.

Creating an Authentication Stage within a V-Realm.

Once you have an understanding of V-Realms, you can move on to creating Authentication Stages in order to integrate NetConnect with your environment to enable user access. This section will cover:

- Active Directory integration
- SMB Authentication
- Internal Authentication
- Multi-Factor authentication

Creating an LDAP Authentication Stage

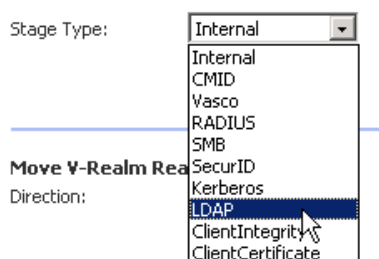
This section describes how to set up NetConnect to authenticate users against an external LDAP server, typically Active Directory. The following main steps are required.

Basic LDAP Configuration for Authentication

To configure the basic settings for an LDAP authentication stage which includes connection and authentication information, follow the below steps. This assumes you have created a V-Realm, as per “Creating a V-Realm” under section 2.2 and follows on accordingly.

- After creating and naming a new V-Realm, select **LDAP** from the Stage Type drop down list box located under Create New Authentication Stage.
- Click **Submit**.

Create New Authentication Stage



The Authentication Stage properties page opens. The basic settings that are required for configuring NetConnect to authenticate users against an external LDAP server can be seen below.

Home
Manage Access
Groups
Applications
Services
Reporting
Monitoring
Customization
System Configuration
Authentication Settings
V-Realm Management
Datastores
Client Integrity
Access Level Management
Global V-Realm Properties
Mobile Device Access

Authentication Stage 1 (Ldap) ?

Type: **Ldap**

Authentication Scope:

Domain:

Username Template:

Reauthentication Interval:

Reauthentication Retries:

Connection settings:

Method:

Host:

Port:

LDAP Version:

Bind settings:

Bind DN:

Bind Password:

Search settings:

Base DN:

Login Attribute:

Search Filter:

Group settings:

Required Group DN:

Excluded Group DN:

Group Member Attribute:

User Member Attribute:

Group Base DN:

Group Name Attribute:

Password changing settings:

Changing Method:

MyDesktop settings:

Workstation Address Attribute:

- Specify the following settings and click **Submit**.

LDAP Settings	Description
Authentication Scope	This field is used to enable Single Sign-On (SSO)/Password Forwarding. Enter a unique name of your choice for the Authentication Scope; for example SSO-01. This name can be referenced when configuring an Application should single sign-on be required.
Domain	Enter the domain which the Active Directory is joined to.
Username Template	The Username template field is used to prefix or postfix a string to the username. This removes the need for end-users to include this information when logging in. For example, if a V-Realm member authenticates against a Domain Controller from a trusted domain, he would need to provide the domain name and username upon each login. Postpending the username template with the name of the trusted domain

	eliminates this requirement. In this case, you would add the domain name before the %USERNAME% template (e.g., mydomainname\%USERNAME%).
Method	<p>Select the connection method that should be used for the connection between NetConnect and LDAP server:</p> <ul style="list-style-type: none"> • LDAP: Provides unencrypted or clear text communication during the session. • LDAPS: An SSL connection is established and then LDAP runs over that SSL connection. • LDAP+TLS: A connection is established and LDAP messages are sent followed by SSL.
Host	Enter either the DNS name or IP address of the LDAP server. DNS name is recommended because this field is used to create entries under Group/LDAP.
Port	Enter the port number of the LDAP server.
LDAP Version	Select the LDAP protocol version of the server
Bind DN	Enter the distinguished name (DN) of a client authorised to search within the LDAP server. If the LDAP server supports anonymous, this field may be left blank.
Bind Password	Enter the password of a client authorised to search within the LDAP server. If the LDAP server supports anonymous, this field may be left blank.
Base DN	Specify the point in the directory hierarchy where a search begins. Enter the base DN (or base Object) from which you want to search.
Login Attribute	Enter the name of the login attribute that contains the user's login name. For example, for Sun Java System Directory Server it's uid. For Active Directory, it's sAMAccountName.
Search Filter	Further narrow down the search starting from the base DN by entering a filter(s). This is helpful if two objects have the same user attribute.

If you intend to enable MyDesktop, populate the **MyDesktop Settings** area accordingly. See 'Configuring MyDesktop Application' within Chapter Three for further details.

Creating an SMB Authentication Stage

Before you begin, have the following SMB server information ready.

- Primary Name: NetBIOS name of your primary SMB server
- Primary IP: IP address of your primary SMB server
- Secondary Name: Name of your secondary SMB server (optional)
- Secondary IP: IP address of your secondary SMB server (optional)

To create an SMB authentication stage, follow the below steps. This assumes you have created a V-Realm, as per "Creating a V-Realm" under section 2.2 and follows on accordingly.

- Choose **SMB** from the Stage Type drop down list box located under Create New Authentication Stage.
- Click **Submit**, as shown below.

Add Stage to Realm 'Realm 3'

Create New Authentication Stage

Stage Type: RADIUS

Internal
 CMID
 Vasco
 RADIUS
SMB
 SecurID
 Kerberos
 LDAP
 ClientIntegrity
 ClientCertificate

« Ready to commit changes »

« Go back to realm list »

The Authentication Stage properties page opens.

Authentication Stage (Realm 3)

Type: **SMB**

Authentication Scope:

Domain:

Username Template:

Reauthentication Interval:

Reauthentication Retries:

Primary Name:

Primary IP:

Secondary Name:

Secondary IP:

Enter the SMB information.

- **Authentication Scope.** If enabling Single Sign On for this stage, enter a name of your choice for example SSO-01. This name can be referenced when configuring an Application should single sign-on be required.
- **Domain.** Enter the domain which the server is joined to.
- **Username Template.** Used to prefix or postfix a string to the username. This removes the need for end-users to include this information when logging in. For example, if a V-Realm member authenticates against a Domain Controller from a trusted domain, he would need to provide the domain name and username upon each login. Postpending the username template with the name of the trusted domain eliminates this requirement. In this case, you would add the domain name before the %USERNAME% template (e.g., mydomainname \%USERNAME%).
- **Primary Name.** NetBIOS name of your primary SMB server
- **Primary IP.** IP address of your primary SMB server
- **Secondary Name (optional).** Name of your secondary SMB server
- **Secondary IP (optional).** IP address of your secondary SMB server

Internal Authentication

The authentication stage named Internal uses NetConnect authentication. Internal authentication is used for NetConnect administrator accounts and is also useful for users that do not use an external authentication server.

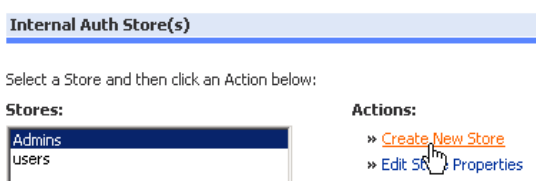
Creating an Internal Database of Users

Prior to creating an Internal Authentication stage, you will require an internal user database – this section will outline how to create and populate a database of internal users.

- From the Administrator Site, navigate to **Authentication Settings > Datastores**.
- Click **Internal Auth. Stores** from the Datastores submenu. The Internal Auth Stores page appears.



- Click **Create New Store**. The Create a new store page appears.

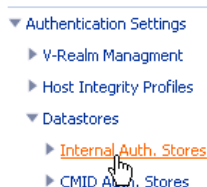


- Enter a name for the group of users you want to add. Note that you can create multiple internal authentication stores.
- Click **Create Store**.

Adding a User

To add a user to an internal database that you have already created:

1. From the Administrator Site, navigate to **Authentication Settings > Datastores**.
2. Click **Internal Auth. Stores** from the Datastores submenu.



The Internal Auth Stores page appears.

3. Choose a store and then click **Get User List**.
4. Under Actions, click **Add User**. The Add a New User page appears for the user group just selected.

Internal Auth. Store: users**Add a New User**

User Name:

Password:

Password Confirm:

- **User Name.** Enter the user's name. The username may have any alphanumeric character, '_' (underscore), space and '.' (dot). It can contain up to 128 uppercase or lowercase characters. Note that user names are not case sensitive, and therefore should not be differentiated by case. For example, a username of "John" is considered to be the same as the user name "john".
 - **Password.** Enter the user's password. Locally stored passwords can contain up to 128 uppercase or lowercase characters. The Password field is case sensitive. The password may have any alphanumeric character, or punctuation marks such as the following English punctuation marks: !"#\$%&'()-~^|\`@[+;*:]<>.,?/_\
 - **Password Confirm.** Enter the user's password again.
- Click Add User.

This database of users must be associated during internal authentication stage. For details, refer to "Creating an Internal Authentication Stage" below.

Creating an Internal Authentication Stage

To create an internal authentication stage, follow the below steps. This assumes you have created a V-Realm, as per "Creating a V-Realm" under section 2.2 and follows on accordingly.

- Choose Internal from the Stage Type drop down list box located under Create New Authentication Stage and then click Submit.

Add Stage to Realm 'Realm 3'**Create New Authentication Stage**

Stage Type:

The Authentication Stage properties page opens.

Authentication Stage (Realm 3) Settings

Type: **Internal**

Authentication Scope:

Domain:

Username Template:

Reauthentication Interval:

Reauthentication Retries:

Reauthentication Retries:

Authentication Store:

- **Authentication Scope.** If enabling Single Sign On for this stage, enter a name of your choice for the; for example SSO-01. This name can be referenced when configuring an Application should single sign-on be required.
- **Domain.** Enter the domain which the server is joined to.
- **Username Template.** Used to prefix or postfix a string to the username. This removes the need for end-users to include this information when logging in. For example, if a V-Realm member authenticates against a Domain Controller from a trusted domain, he would need to provide the domain name and username upon each login. Postpending the username template with the name of the trusted domain eliminates this requirement. In this case, you would add the domain name before the %USERNAME% template (e.g., mydomainname\%USERNAME%).
- **Authentication Store.** Select the name of the group of users that you want to associate with this authentication stage. See 'Creating an Internal Database of Users' for further details.
- Click **Submit**.

Deleting a User from an Internal Database of Users

To delete a user, do the following:

- From the Administrator Site, navigate to **Authentication Settings > Datastores**.
- Select **Internal Auth Stores** from the Datastores submenu.
- Locate and then select the name of the database that contains the user you want to delete and then click Get User List. An example is shown.

Internal Auth Store(s)

Select a Store and then click an Action below:

Stores:

Admins
users

Actions:

- » Create New Store
- » Edit Store Properties
- » [Get User List](#)

- Select the name of the user you want to delete and then click Edit Properties. An example is shown.

Store Name: users

Select a User and then click an Action below:

Users:

newuser

Actions:

- » [Edit Properties](#)

- Select Delete User as shown.

Properties for user: newuser

Change Password

New Password:

New Password Confirm:

Update Password

Delete the selected user

Deleting a Datastore

To delete the entire database of users, do the following:

- Navigate to **Authentication Settings > Datastores..**
- Select **Internal Auth Stores** from the Datastores submenu.
- Select the database that you want to delete and then click **Edit Store Properties**.

Internal Auth Store(s)

Select a Store and then click an Action below:

Stores:



A screenshot of a web interface showing a list of stores. The list has two entries: 'Admins' and 'Users'. 'Admins' is highlighted with a blue background.

Actions:

- » [Create New Store](#)
- » [Edit Store Properties](#)
- » [Get User List](#)

- Click **Delete Store**. A pop up message asks you to confirm that you want to delete this store.
- Select **Yes**. The datastore is deleted.

Two Factor Authentication

The Radius authentication stage can be used to integrate two-factor authentication solutions, providing the solution you wish to incorporate supports Radius authentication. This section will outline the steps in configuring a two-factor authentication stage.

Creating a RADIUS Authentication Stage

The follow assumes you have created a V-Realm, as per “Creating a V-Realm” under section 2.2 and follows on accordingly.

Before you begin, have the following RADIUS server information ready.

Authentication Stage	Description
Primary RADIUS Server IP	IP address of RADIUS server.
Primary RADIUS Secret	Enter the Shared Secret configured on the RADIUS server in this field. The RADIUS Secret is case-sensitive and must match the RADIUS server secret exactly.
Primary RADIUS Port	Enter the port number of the RADIUS server. It is usually 1812 or 1645
Primary RADIUS Timeout	60 seconds is recommended.
Initial Password	(Optional) If using challenge response, you can preconfigure an initial password for use until the RADIUS server sends the challenge. Alternatively, you can configure the Empty Password field
Empty First Password	(Optional) If using challenge response, check this box to eliminate the use of the first password.
Group attribute ID	(Optional) Enter the number that represents the ID of the attribute which contains group membership information. Group membership information <u>_is_</u> space separated list of group names. For example, an attribute named “Role” contains group membership information (such as “Group1 Group2 Group3”) and the numeric ID of “Role” attribute is 123. For this example, the “Group Attribute ID” should be set to 123.
Attributes Encoding	This required field is set to UTF-8 by default. This is the encoding of attribute values (e.g., user name, password, group name).
Secondary RADIUS Server IP	(Optional) IP address of backup RADIUS server.
Secondary RADIUS Port	(Optional) Port of backup RADIUS server.
Initial Password	(Optional) If using challenge response, you can preconfigure an initial password for use until the RADIUS server sends the challenge. Alternatively, you can configure the Empty Password field.

Empty First Password	(Optional) If using challenge response, check this box to eliminate the use of the first password.
Group Attribute ID	<p>(Optional) Enter the number that represents the ID of the attribute which contains group membership information. Group membership information _is_ space separated list of group names.</p> <p>For example, an attribute named "Role" contains group membership information (such as "Group1 Group2 Group3") and the numeric ID of "Role" attribute is 123. For this example, the "Group Attribute ID" should be set to 123.</p>
Attributes Encoding	This required field is set to UTF-8 by default. This is the encoding of attribute values (e.g., user name, password, group name).

- Choose RADIUS from the Stage Type drop down list box located under Create New Authentication Stage.
- Click **Submit**

Create New Authentication Stage

Stage Type:

Internal
CMID
Vasco
RADIUS
SMB
SecurID
Kerberos
LDAP
ClientIntegrity
ClientCertificate

« Ready to commit changes
« Go back to realm list

The Authentication Stage properties page opens.

Authentication Stage (Realm 3)

Type: **RADIUS**

Authentication Scope

Domain

Username Template

Reauthentication Interval

Reauthentication Retries

Primary RADIUS

RADIUS Server IP RADIUS Port (Usually 1812 or 1645)

RADIUS Secret RADIUS Timeout

Initial password Empty First Password ☐

Group Attribute ID Attributes Encoding

Secondary RADIUS

☐ select to include backup server.

RADIUS Server IP RADIUS Port (Usually 1812 or 1645)

RADIUS Secret RADIUS Timeout

Initial password Empty First Password ☐

Group Attribute ID Attributes Encoding

- **Authentication Scope.** If enabling Single Sign On for this stage, enter a name of your choice: for example SSO-01. This name can be referenced when configuring an Application should single sign-on be required.
- **Domain.** Enter the domain which the server is joined to.

- **Username Template.** Used to prefix or postfix a string to the username. This removes the need for end-users to include this information when logging in. For example, if a V-Realm member authenticates against a Domain Controller from a trusted domain, thhe would need to provide the domain name and username upon each login. Postpending the username template with the name of the trusted domain eliminates this requirement. In this case, you would add the domain name before the %USERNAME% template (e.g. mydomainname \%USERNAME%).
- Configure the remaining fields with your specific RADIUS information, as described in the table above.
- Click **Submit**

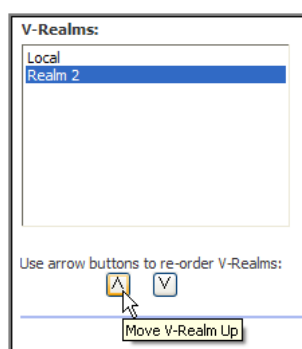
Managing V-Realms

This section describes how to move V-Realms, delete V-Realms, and change the appearance of the V-Realm field.

Re-Ordering V-Realms

To change the location of a V-Realm in the list of V-Realms, do the following.

- From the Administration Site, click **Authentication Settings** and then select **V-Realm Management**.
- Select the V-Realm that you want to move and then use the buttons located under the V-Realm list box to change the list order.



Deleting V-Realms

To delete a V-Realm, do the following.

- Click **Authentication Settings** and then select **V-Realm Management**.
- Select the name of the V-Realm that you want to delete, and then select **Delete V-Realm**.

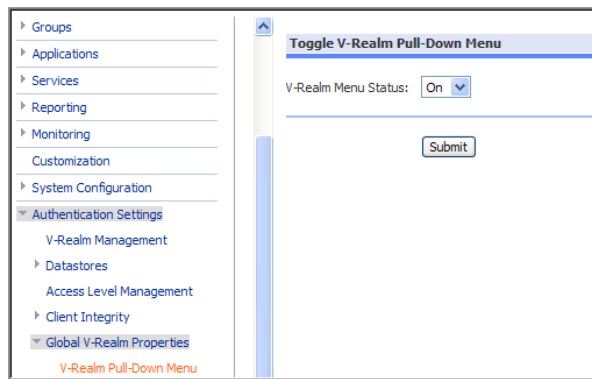


Changing the V-Realm Field Appearance

By default, V-Realms that you created are selected from the V-Realm drop down menu upon log in. Alternatively, you can display the V-Realm Name field which requires end users to know their V-Realm name and type it into the V-Realm Name field.

To change the V-Realm field to a text box or to a drop down menu, do the following.

- Navigate to **Authentication Settings > Global V-Realm Properties > V-Realm Pull-Down Menu**.
- The Toggle V-Realm Pull-Down Menu page appears.



- Select **Off** if you want a V-Realm list box. Select **On** if you wish to have the V-Realm menu as a drop down list.
- Click Submit.

Chapter Three. Application Configuration

This chapter covers a selection of application types that can be published, as well as specific features that can be configured within these applications. NetConnect can be utilised to publish RDP, SSH, Telnet or VNC applications via HTML5 and further configured for enhanced functionality. This chapter will cover:

- Creating an HTML5 RDP application.
- Creating a MyDesktop application.
- Creating an SSL/Telnet application.
- Creating a VNC application.
- HyperDrive.
- Assigning access to applications.
- Printing from an application.
- Assigning multiple servers to a single application.

About RDP Applications.

When you “create” an application you are actually creating a logical pointer to the real application on the remote server.

Microsoft Windows applications must be installed on a Microsoft Windows 2008/2012/2016 server with Remote Desktop Services (formerly Terminal Services), and must be compatible with MS Terminal Server and RemoteApp.

About Microsoft Licensing.

Microsoft Licensing is invoked when a user launches an application that is configured to run from a Microsoft Terminal Server. Each application that is launched initiates a new terminal server session. Users are required to follow the licensing requirements as set forth by Microsoft (generally Per User CAL's).

3.1 HTML5 RDP Applications.

This section describes how to create a typical HTML5 RDP application, and provides an overview of the configuration options. Connections can be configured for access to specific desktops, applications or servers as required.

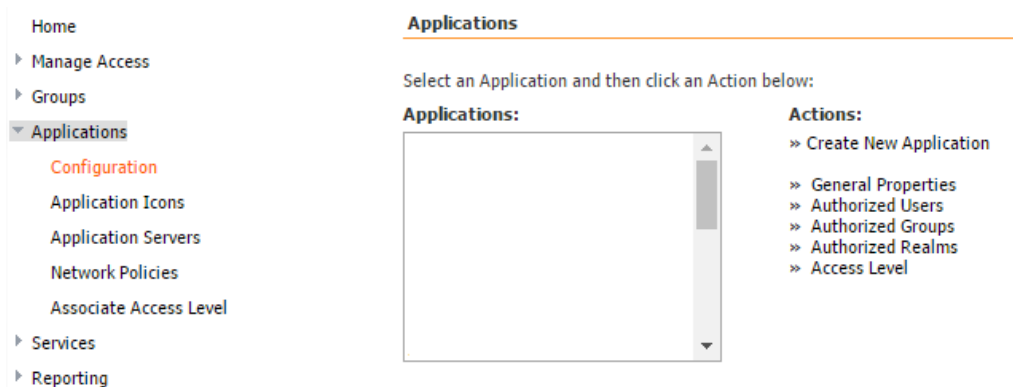
Please note, for an application to be accessible from a Windows Server via HTML5, a specific group policy must be configured. Note, this group policy must be configured whether you are publishing the server desktop via RDP HTML5 or a specific server-based application.

The **‘Allow Remote Start of Unlisted Programs’** group policy can be found in the following location within the destination servers group policy editor:

Computer Configurations > Administrative Templates > Windows Components > Remote Desktop Services > Remote Session Host > Connections

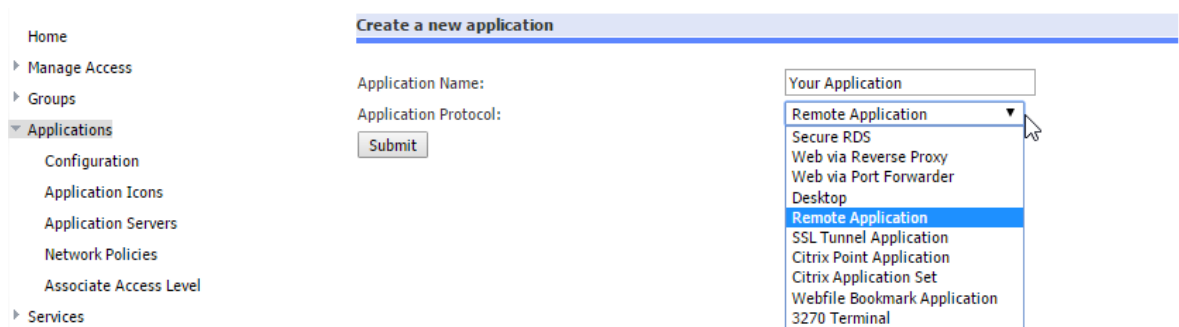
Creating an HTML5 RDP Application

- From the Admin page, click **Applications > Configuration**. The Applications page opens.
- Select **Create New Application**.



The 'Create a new application' page appears.

- Enter the application name in the **Application Name** field.
- Select Remote Application from the **Application Protocol** drop-down menu.



- Click **Submit**. The General properties page is displayed.

General Properties

Desktop

Application Name: Desktop

Application Type: Remote Application

Application Icon: rdpapp.gif

Remote Application Type: ☒ Regular RDP ☐ MyDesktop

Full Address: OR ☐ Allocate Application Servers ☐ User Select Address

TS RemoteApp Support: Off

Application Path:

Working Directory:

Color Depth: Device default

Application Size: ☒ Full Screen ☐ Workarea on Linux, Full screen on others ☐ 640x480 ☐ 800x600 ☐ 1024x768 ☐ Custom

Remote Protocol: RDP

HTML5 Client: On

- **Application Name.** Enter a name such as Word for the HTML5 application that you are creating.

Note: use a descriptive name to make it easier to identify when it comes time to apply the policies.

- **Application Type.** Pre filled from previous page but is not editable.
- **Application Icon.** Click *Browse* to choose an icon for the application that will be displayed on users' WebTops or leave the default (Customised Icons can also be uploaded).
- **Remote Application Type:** Leave this as the default 'Regular RDP' unless you are creating a MyDesktop application specifically.
 - See 'Configuring a MyDesktop Application' below for further information.
- **Full Address.** Enter the server address (either hostname or IP).
 - Note, **DNS Caching** must be set to 'Off' if using a hostname. Refer to 'DNS Cache' within section 4.2 System Maintenance.
 - **Allocate Application Servers.** Selected if you wish to utilise a pool of application servers, refer to the 'Utilising Multiple Server for a Single Application' section below for further information.
 - **User Select Address.** Select if you wish to allow users to enter a specific destination IP or Hostname at the point of connection. It is recommended that your DNS suffix is configured within NetConnect if users will be access devices by Hostname. Refer to 'DNS Suffix' within section 4.2 System Maintenance.
- **TS RemoteApp Support.** Set to 'Off'.
- **Application Path.** If publishing an application, enter the full path of the application. For example, C:\Program Files\Microsoft Office\Office15\winword.exe.
- **Working Directory** (Optional). Enter the location of the folder that contains the application or related information.
- **Color Depth.** Device default is appropriate for most cases.
- **Application Size.** Choose the screen area in which the application operates. Full Screen is appropriate for most cases.
- **Remote Protocol.** Select the protocol you wish to use to connect to the application.

- **RDP.** Default, the most commonly used protocol when connecting to a Windows based application or end user computer.
- **VNC.** Predominantly used for connections to instances which do not support RDP, for example Windows Home Edition PCs. This option is dependent on the destination PC running a version of VNC. See section 3.3 'Configuring a VNC Connection' for further details.
- **SSH.** See section 3.2 'Configuring an SSH/TelNet Connection' for further details.
- **TelNet.** See section 3.2 'Configuring an SSH/TelNet Connection' for further details.
- **HTML5 Application.** The default option for Remote Applications. This can be changed to 'Off' to use the legacy Java Port Forwarder.
- **Modify.** The new application is added to the system.

Please refer to 'Advance Application Configuration' for additional configuration options.

Configuring a MyDesktop Application

MyDesktop enables users to access their physical desktops/laptops from remote locations. MyDesktop uses LDAP to retrieve the user information; under a typical implementation an administrator would nominate a field within the Active Directory to act as a reference point for NetConnect to lookup the individual users' workstation static IP address or hostname. The administrator then populates this Active Directory attribute with the appropriate information for each user, configures NetConnect to reference the chosen attribute.

Please note, MyDesktop will only be accessible to users within a V-Realm that has LDAP Authentication stage configured.

There are three main steps required to set up MyDesktop Access:

- Prepare LDAP for retrieval of user information.
- Create a MyDesktop application type.
- Allow users to access their MyDesktop application type from their WebTop.

Note, **DNS Caching** must be set to 'Off' if using a hostname. See 'DNS Caching' within section 4.2 System Administration for further details.

Prepare LDAP for Retrieval of User Desktop Information

To set up LDAP to retrieve the user specific desktop details, follow these steps. This section assumes an LDAP Authentication Stage has been configured against a V-Realm. See 'Configuring an Authentication Stage Within a V-Realm' under section 2.2 for further details around Authentication Stages.

- Within your LDAP, identify an available user attribute which is not currently in use. Typically, the telephone number attribute is utilised (facsimileTelephoneNumber).
 - An LDAP administrator tool could be utilised to browse your LDAP tree to assist in locating an appropriate attribute should this attribute be in use.
- For each user who you wish to assign MyDesktop to, you will need to enter either the IP address or hostname of the user's PC in the attribute field.

Once an available attribute has been identified:

- Navigate to **Authentication Settings > V-Realm Management**.

- Select the V-Realm against which MyDesktop is being configured and click **Edit V-Realm Stages**.
- Highlight the LDAP stage and click **Edit Stage**.
- Under the MyDesktop heading, enter the relevant LDAP attribute within the **Workstation Address Attribute** field.



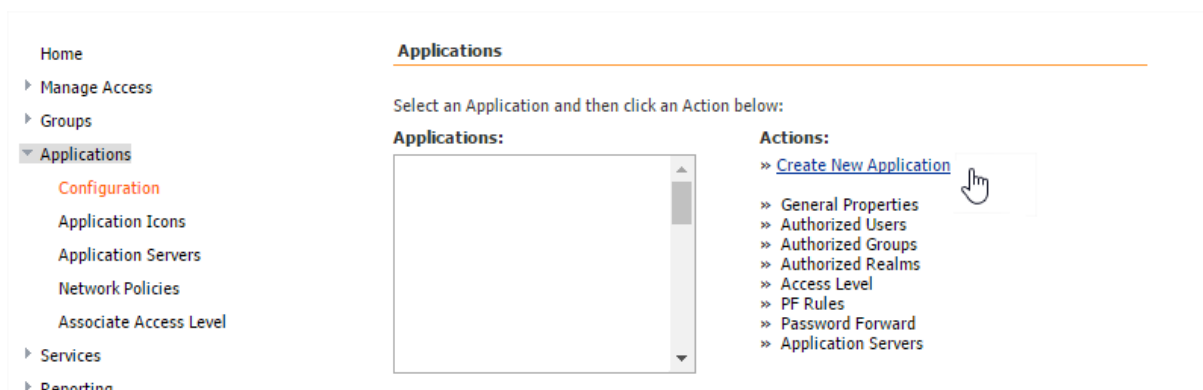
MyDesktop settings:

Workstation Address Attribute

- Click **Submit**.

To create a MyDesktop application:

- Navigate to **Applications > Configuration**.
- Select **Create New Application**.



Home

- Manage Access
- Groups
- Applications**
 - Configuration**
 - Application Icons
 - Application Servers
 - Network Policies
 - Associate Access Level
- Services
- Reporting

Applications

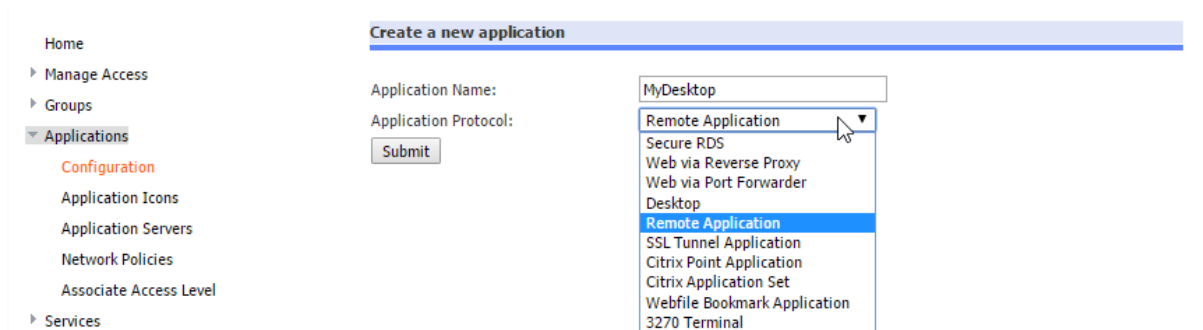
Select an Application and then click an Action below:

Applications:

Actions:

- » [Create New Application](#)
- » General Properties
- » Authorized Users
- » Authorized Groups
- » Authorized Realms
- » Access Level
- » PF Rules
- » Password Forward
- » Application Servers

- For **Application Name**, enter a name such as My Desktop and select Remote Application as the Application Protocol.



Home

- Manage Access
- Groups
- Applications**
 - Configuration**
 - Application Icons
 - Application Servers
 - Network Policies
 - Associate Access Level
- Services

Create a new application

Application Name:

Application Protocol:

Remote Application

Secure RDS

Web via Reverse Proxy

Web via Port Forwarder

Desktop

Remote Application

SSL Tunnel Application

Citrix Point Application

Citrix Application Set

Webfile Bookmark Application

3270 Terminal

NOTE: Use a descriptive name to make it easier to identify when it comes time to apply the policies.

- Click **Submit**. The General properties page is displayed
- **Remote Application Type** should be set to 'MyDesktop'
- **Remote Protocol** should be set to 'RDP'
- **HTML5 Client** should be set to 'On'

The screenshot shows the 'General Properties' window for an application named 'MyDesktop'. The left sidebar contains a navigation menu with 'Applications' selected. The main area has the following fields and options:

- Application Name:** MyDesktop
- Application Type:** Remote Application
- Application Icon:** rdpapp.gif (with a 'Browse...' button)
- Remote Application Type:** ☒ MyDesktop, ☐ Regular RDP
- Full Address:** (empty text field) OR ☐ Allocate Application Servers ☐ User Select Address
- TS RemoteApp Support:** Off
- Application Path:** (empty text field)
- Working Directory:** (empty text field)
- Color Depth:** Device default
- Application Size:** ☒ Full Screen, ☐ Workarea on Linux, Full screen on others, ☐ 640x480, ☐ 800x600, ☐ 1024x768, ☐ Custom
- Remote Protocol:** RDP
- HTML5 Client:** On

At the bottom are three buttons: 'Modify', 'Delete this app', and 'Make a Copy'.

Please refer to 'Advance Application Configuration' for additional configuration options.

3.2 Configuring an SSH or Telnet Application.

Providing contactors or system administrators with access to Linux or legacy based hardware can be a cumbersome process. Networks may have switches, routers and hubs, a PABX or other device which can be accessed using SSH or Telnet. NetConnect 8.3 introduces the option for connecting to devices via SSH or Telnet via HTML5 in order to provide clientless access.

To create an SSH application:

- Navigate to **Applications > Configuration**.
- Select **Create New Application**.

The screenshot shows the 'Applications' configuration page. The left sidebar has 'Applications' selected. The main area has the following elements:

- Header:** Applications
- Instruction:** Select an Application and then click an Action below:
- Applications:** A large empty box for listing applications.
- Actions:**
 - [Create New Application](#) (with a hand cursor icon pointing to it)
 - [General Properties](#)
 - [Authorized Users](#)
 - [Authorized Groups](#)
 - [Authorized Realms](#)
 - [Access Level](#)
 - [PF Rules](#)
 - [Password Forward](#)
 - [Application Servers](#)

The 'Create a new application' page appears.

- Enter the application name in the **Application Name** field.
- Select Remote Application from the **Application Protocol** drop-down menu.

Click **Submit** and the General Properties page will appear.

- **Application Name.** Enter a name such as Word for the HTML5 application that you are creating

Note: use a descriptive name to make it easier to identify when it comes time to apply the policies.

- **Application Type.** Pre filled from previous page but is not editable.
- **Application Icon.** Click *Browse* to choose an icon for the application that will be displayed on users' WebTops or leave the default (Customised Icons can also be uploaded).
- **Full Address.** Enter the IP address of the SSH or Telnet server.
 - **User Select Address.** Select if you wish to allow users to enter a specific destination IP or Hostname at the point of connection.
- **Remote Protocol.** Select SSH or Telnet.

Note, **Server Port** will be populated with the default port for SSH (Port 22) or Telnet (Port 23). If you have used a custom port, change this in the server port field.

Finally, select **Modify** to save your changes and create the application. Once the application has been created, it will need to be assigned to a user, group or V-Realm in order to enable access. See 'Authorising Access to Applications' within section 3.4.

3.3 Configuring a VNC Application

VNC or **Virtual Network Computing** is a graphical desktop sharing system that allows the remote access of another PC using the **Remote Frame Buffer Protocol** (RFB). This protocol works similar to that of the more commonly known desktop sharing protocol of **RDP**.

VNC applications can be configured within NetConnect to provide access to destinations which do not support RDP, for example Windows Home Edition. Additionally, publishing applications via VNC allows for screen sharing, which is not currently available with RDP protocol within NetConnect. To enable a VNC connection via NetConnect:

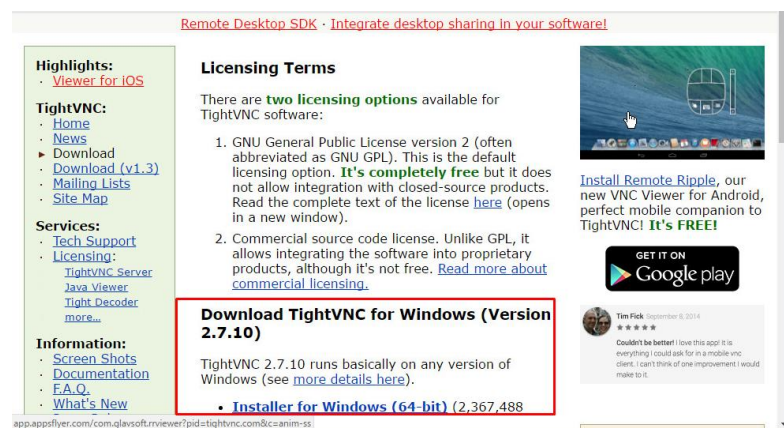
- The destination machine must have a VNC server client installed, configured and running.
- A VNC application must be configured within NetConnect.

This section will act as a guide for installing and configuring the VNC server on the destination machine, as well as the process of creating a specific VNC application on the NetConnect System.

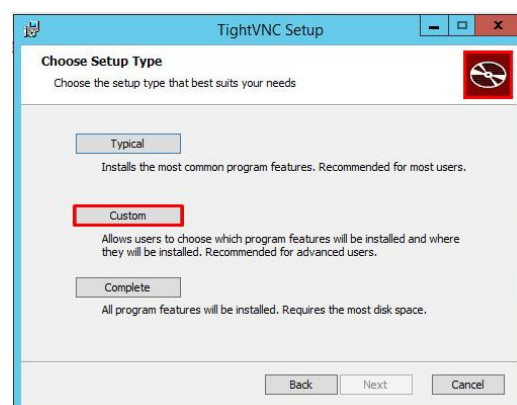
Installing the VNC Client

Before the application can be created and installed on the NetConnect environment, the VNC client must first be created and configured. In order to achieve this, please follow the below walkthrough. Please note that this must be installed on the server or PC that is to be remotely accessed;

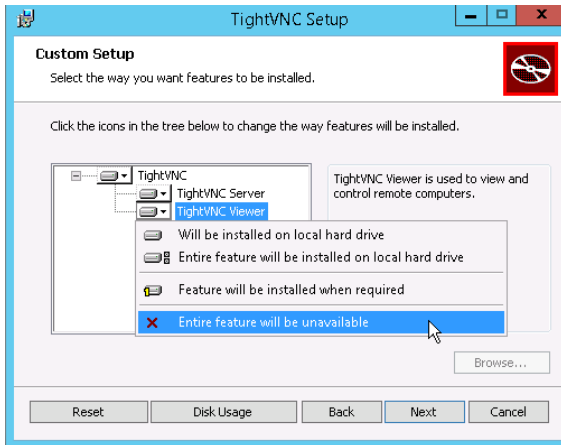
- Download the VNC server client.
 - For this example, we will be using the x64 installer for Tight VNC. This can be found from the following URL: <http://www.tightvnc.com/download.php>.



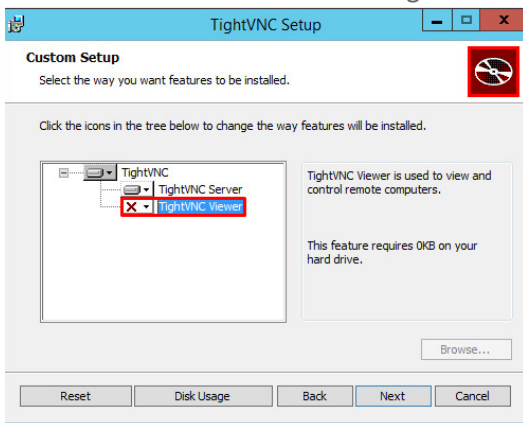
- Once the program has been downloaded, you will need to run the installer. Follow the installer to the below screen and select **Custom** setup type.



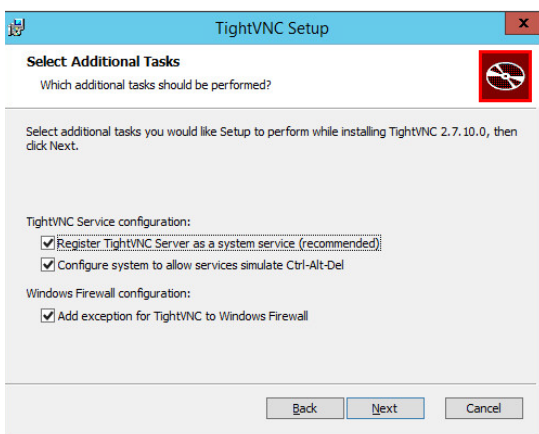
1. Select the drop down list next to **TightVNC Viewer** and select the option **Entire Feature will be Unavailable**.



2. Once this option has been selected, please confirm that the TightVNC Viewer has now been disabled before continuing with this guide.



3. You will be asked if you require any additional tasks to be setup during the install. Please ensure that all boxes are checked and select next.



4. Follow the remaining steps on the setup wizard to complete the installation. Before the install has been completed, you will be prompted to configure a password for authentication. Please make a note of these as they will be required for creating the application from within NetConnect. If the password used is the same as the password for the account that you will be accessing the session from, Password Forwarding can be configured within NetConnect for a convenient end-user experience.

TightVNC Server: Set Passwords

Please protect your TightVNC Service. Make sure to enter a password for remote access. Also, it might be a good idea to use administrative password on multi-user systems.

Password for Remote Access

☐ Do not change
☐ Do not use password protection (DANGEROUS!)
☒ Require password-based authentication (make sure this box is always checked!)

Enter password:

Confirm password:

Administrative Password

☐ Do not change
☐ Do not use password protection
☒ Protect control interface with an administrative password

Enter password:

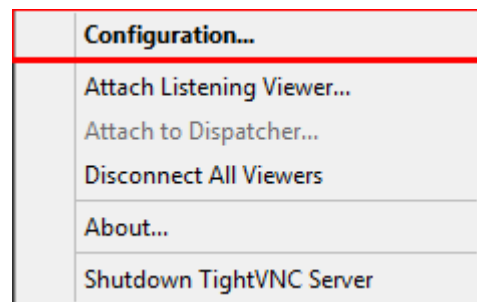
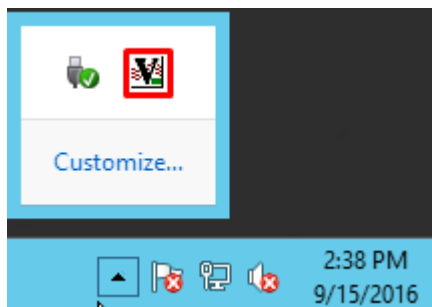
Confirm password:

OK

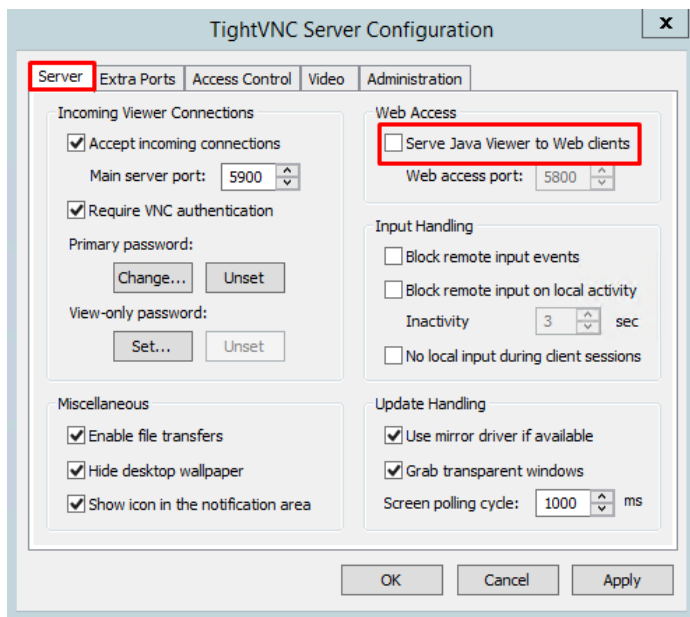
Configuring the VNC Server

Once the VNC client has been installed, several configuration changes should be carried out prior to creating and testing an application on NetConnect.

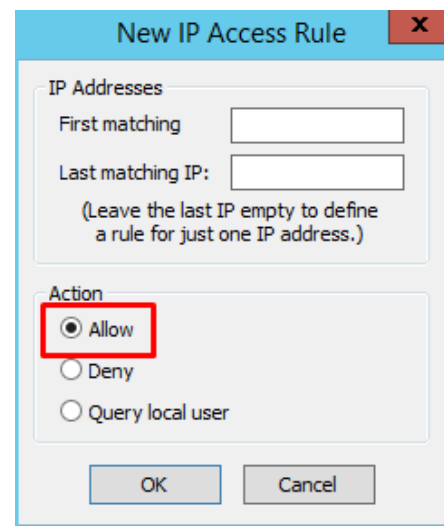
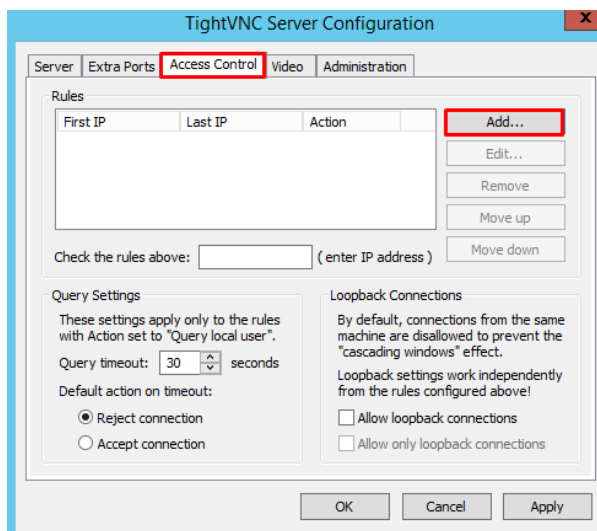
- Open the Notification tray, located at the bottom of the tray and right – click the VNC tab and select configuration.



- On the **Server** tab, ensure that the **Serve Java Viewer to Web Clients** is unchecked. Please also note the port number as this will be required for the NetConnect application later on.

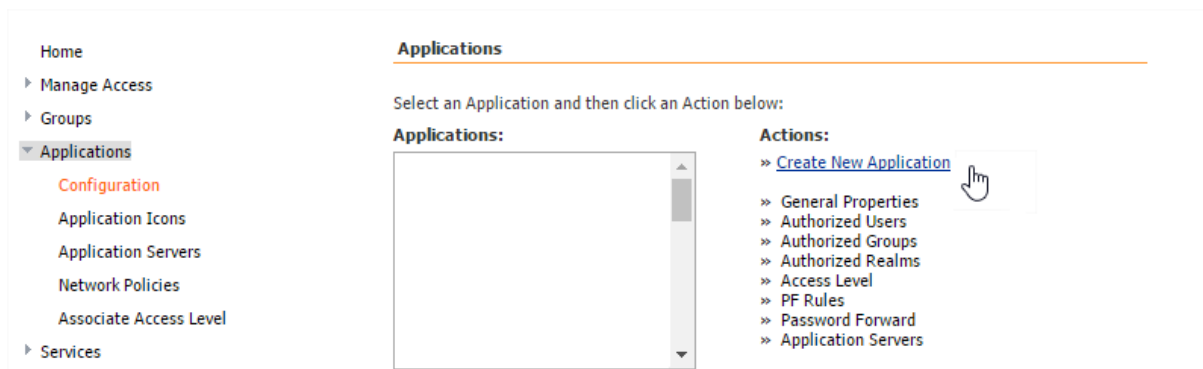


- Finally navigate to the **Access Control** tab and add the IP address of the NetConnect Environment. Please ensure that the **Action** has been selected to **Allow**. We recommend this step, as it will ensure that only connections from the NetConnect server will be accepted.



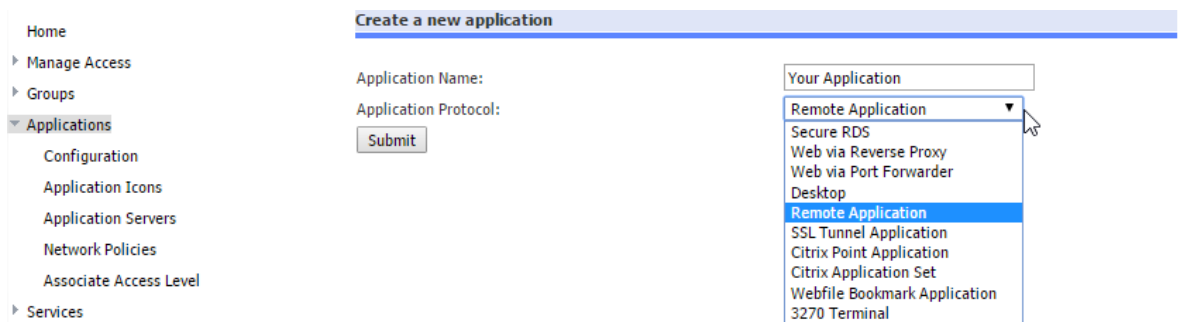
Configuring the VNC Application in NetConnect
To create a VNC application:

- Navigate to **Applications > Configuration**.
- Select **Create New Application**.



The 'Create a new application' page appears.

- Enter the application name in the Application Name field.
- Select Remote Application from the Application Protocol drop-down menu



Click **Submit** and the General Properties page will appear.

- **Application Name.** Enter a name such as Word for the HTML5 application that you are creating

Note: use a descriptive name to make it easier to identify when it comes time to apply the policies.

- **Application Type.** Pre filled from previous page but is not editable.
- **Application Icon.** Click *Browse* to choose an icon for the application that will be displayed on users' WebTops or leave the default (Customised Icons can also be uploaded).
- **Full Address.** Enter the IP address of the server that the VNC server was built on.
- **Remote Protocol.** Select VNC.

Note, **Server Port** will be populated with the default port for VNC (Port 5900). If you have used a custom port this field will need to be modified.

General Properties

10 - VNC Win10E SSO

Application Name: 10 - VNC Win10E SSO

Application Type: Remote Application

Application Icon: rdpapp.gif

Remote Application Type: ☒ Regular RDP ☐ MyDesktop

Full Address: 10.2. ☐ OR ☐ Allocate Application Servers ☐ User Select Address

TS RemoteApp Support: Off ▼

Application Path:

Working Directory:

Color Depth: Device default ▼

Application Size: ☐ Full Screen ☐ Workarea on Linux, Full screen on others ☐ 640x480 ☒ 800x600 ☐ 1024x768 ☐ Custom

Remote Protocol: VNC ▼

HTML5 Client: On ▼

Advanced Properties

Server Port: 5900

Select **Modify** to save your changes and create the application. Once the application has been created, it will need to be assigned to a user, group or V-Realm in order to enable access. See 'Authorising Access to Applications' within section 3.4.

Finally once the application has been assigned and launched, it will prompt you for a password. Simply insert the password that was assigned to the VNC client earlier in the installation. Note, this dialogue box will not be displayed if Password Forwarding has been configured.

Password required

If you have forgotten your password, please contact your system administrator

Enter your password here

Limitations of VNC with NetConnect

When using the VNC feature with NetConnect, there are a few limitations that must be taken into consideration. One of these considerations includes screen resolution. When using the VNC feature, the screen resolution will match that of the remote server, so this may cause issues if connecting through mobile devices. Additionally, printing is not available via VNC connections.

3.4 Advanced Application Configuration.

Advanced Properties.

When configuring an RDP application, several additional configuration options can be utilised to provide additional functionality.

Below is an overview of the commonly utilised options. Note, option availability varies depending on the applications Remote Protocols.

The screenshot shows the 'Advanced Properties' configuration window. On the left is a navigation pane with categories: Home, Manage Access, Groups, Applications (selected), Services, Reporting, Monitoring, Customization, System Configuration, and Authentication Settings. Under 'Applications', 'Configuration' is selected, showing sub-items: Application Icons, Application Servers, Network Policies, and Associate Access Level. The main area displays the following settings:

- Server Port: 3389
- Domain: (empty text field)
- Automatic Reconnection Enabled: On
- Maximum Reconnection Attempts: 20
- Compression: On
- Plugin Lists: (empty text field)
- Apply Windows key combinations: Only when in fullscreen mode
- Remote Computer Sound: No sound
- Disable CTRL+ALT+DEL: On
- Display Connection Bar: On
- Disable Themes: Off
- Disable Menu Animation: On
- Disable Full Window Drag: On
- Disable Wallpaper: On
- Redirect Clipboard: Off
- Redirect Smart Cards: On
- Virtual Drive Upload: Off
- Font Smoothing: Off
- NLA Authentication: Any
- Ignore Certificates for NLA Authentication: On
- Keyboard Type: FailSafe
- Redirect COM Ports: Off
- Redirect Drives: Off
- Redirect Printers: On
- Bitmap Cache Persist Enable: On
- Bitmap Persistence: On
- Bitmap Cache Size: 1500
- 8bpp Bitmap Persistent Cache Size: 10
- 16bpp Bitmap Persistent Cache Size: 20
- 24bpp Bitmap Persistent Cache Size: 30
- Bitmap Persist Cache Locations: %LOCAL_APPDATA%\Mi
- Monitor Span: Off
- Multi monitor support: Off
- Show server authentication warning: On
- Administrative console: Off

Option	Description
Server Port	The port used to communicate to your application. This field will be populated with a default port depending on the Remote Protocol selected for the application, however this can be modified if required.
Domain	Enter the domain on which the server you are connecting to resides.
Remote Computer Sound	Set to 'Play Sounds on Remote Computer' to allow sounds to play through the computer you are connecting to. Set to 'Play Sound on Local Computer' to pass sounds through to the device you are connecting from. Set to 'No Sound' if you do not require any sound.
Virtual Drive Upload	Set to 'On' to enable Hyper Drive document upload functionality. See 'Enabling HyperDrive' section below for further information.

Font Smoothing	Set to 'On' to enable Font Smoothing for improved font quality. Please note, enabling Font Smoothing will increase bandwidth usage and may impact session performance for low-bandwidth connections.
NLA Authentication	Set to 'On' if connecting to a server/PC which has NLA enabled* Set to 'Off' if connection to a server/PC which does not have NLA enabled Set to 'Any' if you are unsure of the NLA settings of the endpoint, or have a mixed environment*.
Ignore Certificates for NLA Authentication	Set to 'On' if utilising NLA Authentication
Keyboard Type	Can be sent to a number of formats to assist with key inputs on keyboards. 'Failsafe' is the best option for multi-lingual environments, or when users can switch input methods. Other options include: <ul style="list-style-type: none"> • Swedish qwerty layout • French azerty layout • Belgium azerty layout • English US qwerty layout • Italian qwerty layout • German qwertz layout • Japanese qwerty layout
Redirect Printers	Set to 'On' to enable local printing from sessions. See 'Printing From NetConnect' within section 3.4 for further details.
Clipboard Redirection	See 'Copy & Paste (beta)' section below.

*Password Forwarding must be configured for any application with NLA set to 'On' or 'Any'.

Copy & Paste (beta).

Release 8.4.0 introduces our **beta** copy & paste functionality. By enabling Keyboard Redirection on a Remote Application configured for HTML5, basic lines of text can be passed between the local and remote sessions. It is important to note that this feature is currently in Beta mode, and therefore user expectations should be set accordingly; formatting (inclusive of carriage returns) is not passed through. Functionality varies across browsers, we recommend using Chrome with the **Clipboard Permissions Manager*** plugin installed or Internet Explorer.

Below is a list of supported browsers and expected behaviour:

Browser	Copy Text In	Copy Text Out	Carriage Return In	Carriage Return Out	Formatting In	Formatting out
Internet Explorer	Yes	Yes	No	No	No	No
Chrome (with add in)*	Yes	Yes	No	Yes	No	No
Chrome (without add in)	No	Yes	No	Yes	No	No
Firefox	No	Yes	No	No	No	No
Edge	No	Yes	No	No	No	No

* <https://chrome.google.com/webstore/detail/clipboard-permission-manager/ipbhneanpgkaleihlknhjiaamobkceh?hl=en>

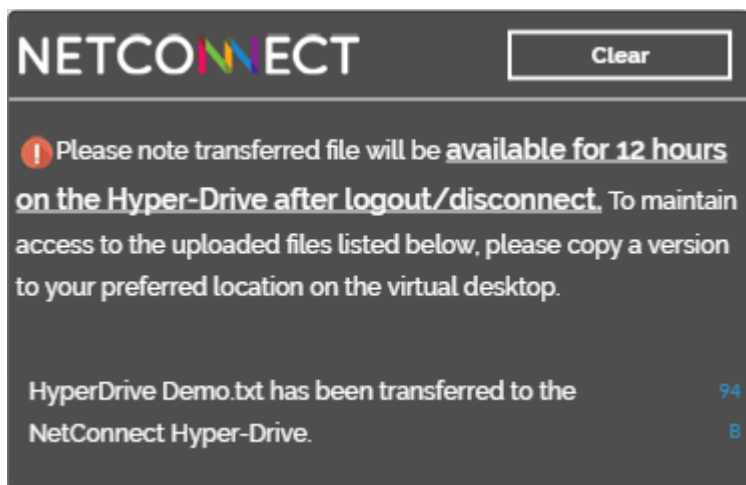
Enabling HyperDrive.

Certain applications or servers are geared towards utility, in that once authenticated, a user is trusted to interact with the company's assets in a responsible manner. Additionally, some users require applications on dedicated servers to perform resource intensive processes – in this situation, they may need to send raw data to the server. HyperDrive has been developed to meet this requirement via NetConnect.

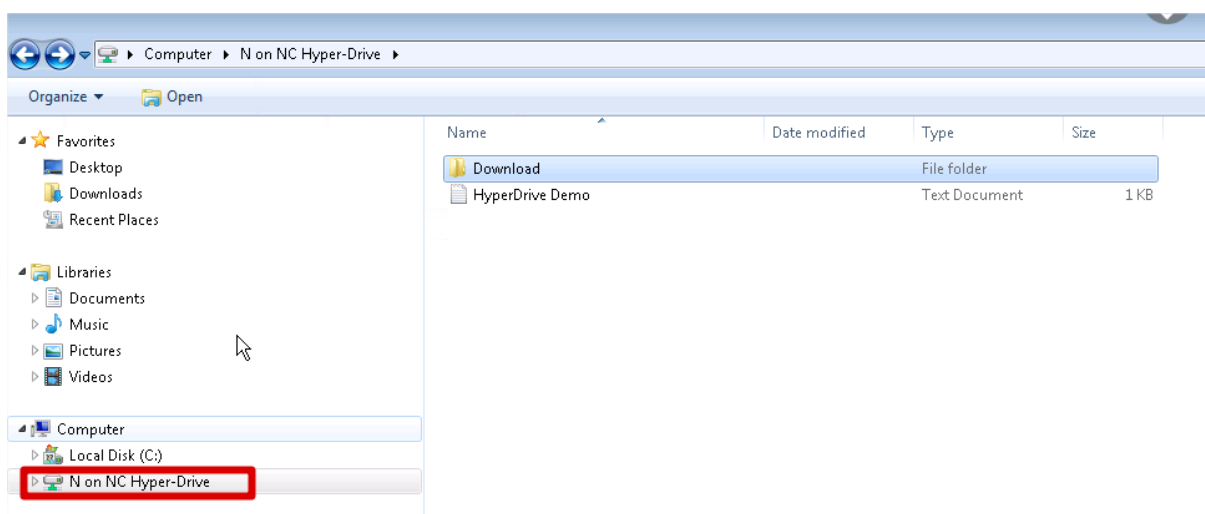
By using the storage available on the NetConnect server, each user will have a temporary storage area available across all applications where the HyperDrive enabled.

Once HyperDrive is enabled, users will be able to drag and drop items into their remote sessions. The files will reside within the NetConnect server, and be accessible via the HyperDrive which will appear as a local drive within the remote session. Please note, the HyperDrive is only a temporary storage area, and users should be trained to move their files from this location to the required destination immediately after the files have been uploaded. The HyperDrive will purge all files within three business days of the data being transferred or when the NetConnect server is rebooted.

When a user moves a file into the HyperDrive, they are presented with the below message:



Once the transfer is complete, files will be available directly within the HyperDrive location.



To enable HyperDrive, you will need to ensure the 'Virtual Drive Upload' flag is set to 'On' within the Advanced Properties of a specific application. Note, HyperDrive is available for RDP HTML5 applications only.

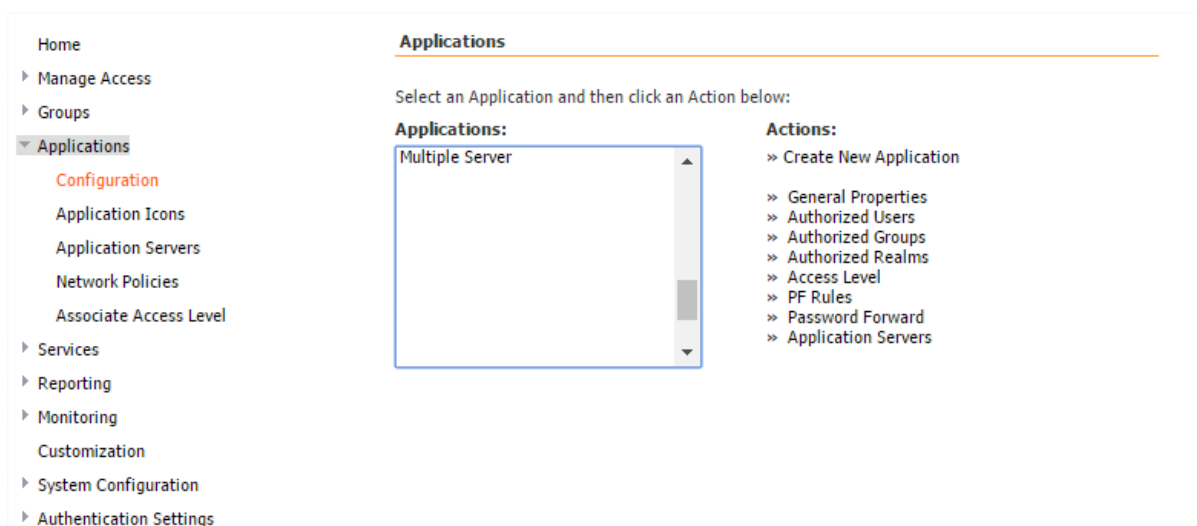
Please note, the HyperDrive feature is made for Business As Usual (BAU) data transfers, and as a point of interconnection between otherwise disconnected resources. As such, it is not suited to large data migrations. HyperDrive utilises the NetConnect server HDD space, and as such we recommend the NetConnect server space is expanded to allow for expected usage and monitored on an ongoing basis.

Setting Up Single Sign On (SSO) via Password Forwarding.

If your back end application servers require users to enter credentials for access, you can simplify the log in process by setting up password forwarding. With password forwarding, once users log in, they can access back end application servers without having to enter credentials. In order for Single Sign On to be enabled, the Authentication Scope and Domain fields must be completed within the specific V-Realms Authentication Stage (see section 2.3 for further details). Password Forwarding can be configured for RDP and VNC applications.

Please note that Password Forwarding must be configured for applications which have NLA Authentication set to 'On' or 'Any'.

- Navigate to **Applications > Configuration**
- Select the name of the application that you wish to enable SSO and click **Password Forward**.



- **Authentication Scope.** Enter the Authentication Scope you created as part of authentication configuration (see “Creating an Authentication Stage within a V-Realm”) enter the same name that was entered in the authentication configuration in this field. This entry must match exactly.
- **Domain Name Forwarding.** Set to 'On'
- Click **Update** to complete the process.

Home

- Manage Access
- Groups
- Applications
 - Configuration
 - Application Icons
 - Application Servers
 - Network Policies
 - Associate Access Level
- Services
- Reporting
- Monitoring
- Customization
- System Configuration
- Authentication Settings

Password Forwarding for '03 - RDP Win8E -NLA'

Authentication Scope: SSO-001

Domain Name Forwarding: On

Update

[« Go back to Application listing](#)

Printing

Overview

NetConnect Release 8 introduces a revised approach to printing, with an emphasis on simplicity and cross-platform support. With this new release, documents can be printed from the Remote session to a locally assigned printer, and can also be saved locally.

Some of the benefits include:

- Print and save documents from a remote session to a local environment
- Simple and easy to use

Please note, two-click support for printing is available for Chrome, FireFox and Safari. While printing is supported within Internet Explorer and Microsoft Edge, additional steps are required.

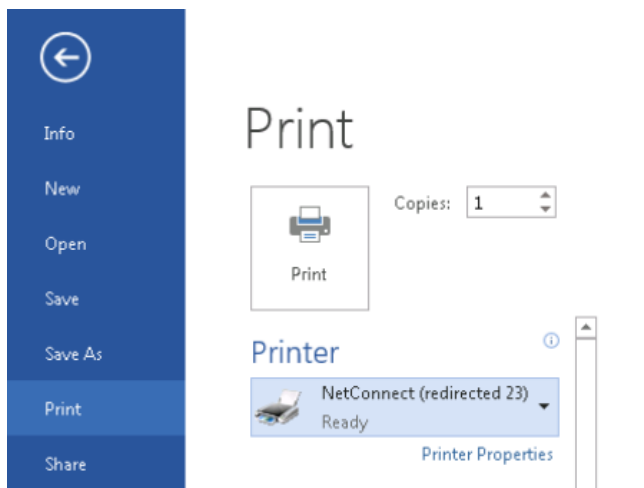
Requirements

- **Redirect Printers** flag set to 'On' within RDP connection applications Advanced Properties.
- Pop-ups must be allowed from your assigned NetConnect URL within your browser to enable two-click printing (Chrome, FireFox and Safari only).

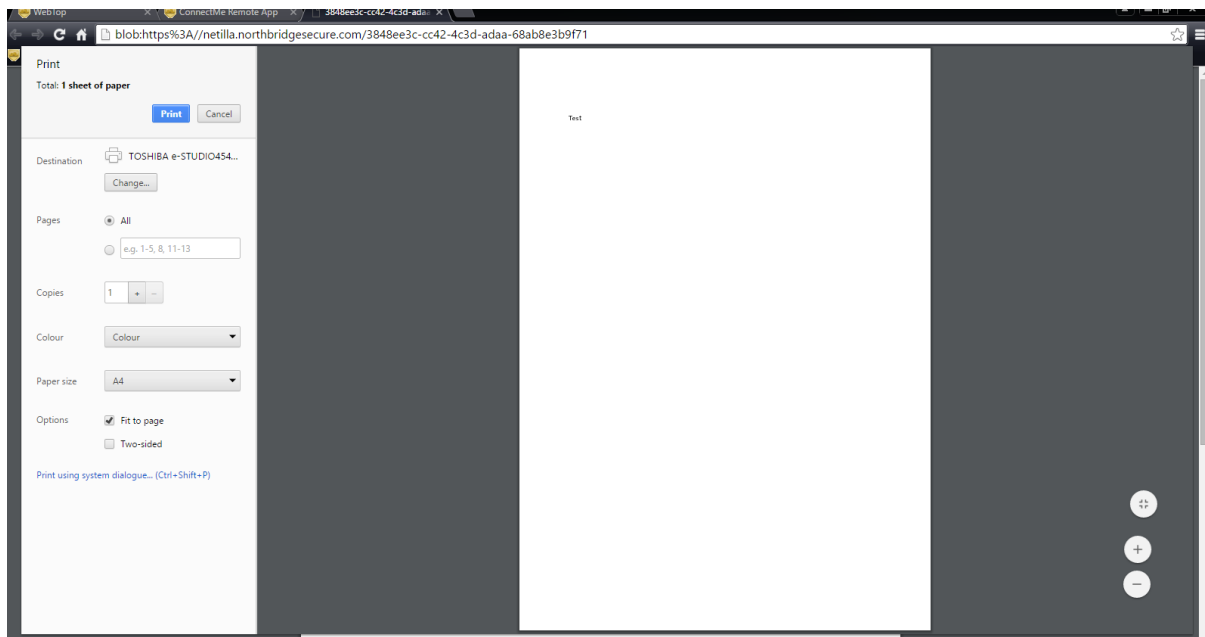
How to Configure and Print While Using NetConnect

This section assumes the application being used has been configured with Printing Redirection. This setting can be located within the 'Advanced Properties' of the application. Please refer to 'Advanced Properties' within section 3.4 for further details.

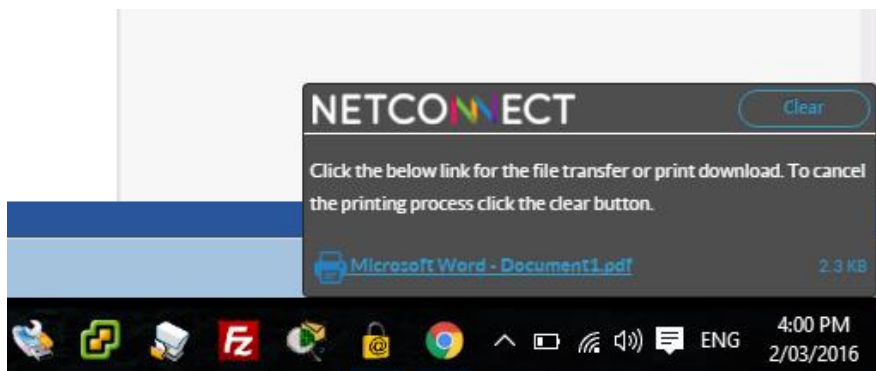
Providing Printing Redirection is configured, the user will be presented with a 'NetConnect (redirected)' printer within their remote session. To print locally, select the print option within the program.



Once the user selects print, a separate tab will open and display an in-browser PDF viewer (Chrome, FireFox & Safari only) and the user will be taken directly to the Print Preview page where they can either print to their default printer, or select an alternative printer. Please note, this stage is not currently supported on Internet Explorer or Edge browsers due to browser imposed limitations; users will need to print as described below.



An option to download a PDF copy of the printed page will be presented to the user in the lower right hand corner of their session. If the hyperlink is clicked, a .pdf version of the document is opened locally using the local default PDF viewer; users connecting from either Internet Explorer or Microsoft Edge can print from their local PDF application. This message can be dismissed by clicking 'Clear'.



Troubleshooting

I can download a local copy but the print tab does not open?

Please note that the printing feature is not currently supported in Internet Explorer and Microsoft Edge. If running in Chrome, FireFox or Safari please ensure that pop-ups from your NetConnect URL are unblocked.

Is it possible to set NetConnect Redirected as the default Printer?

It is possible to set NetConnect as the default printer but this must be changed within the Group policy settings on the App Server. The 'allow redirected printers as default' must be selected and enabled.

Utilising Multiple Servers for a Single Application.

Overview

NetConnect 8.3 and above allows for a round robin server pooling mechanism in order to publish a single application from multiple servers. Customers may find a single application has significantly more usage than others, and therefore are required to balance the load over multiple servers.

In Fig.1 the example business has servers for individual business units. All business units depend on a CRM to capture processed information. Two business unit servers are underutilised, while the CRM server is running at full capacity.

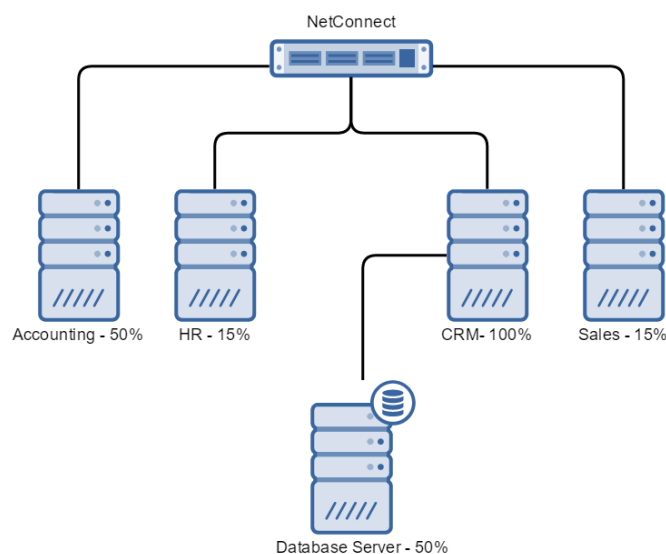


Fig.1.

Under this scenario, the Sales and HR servers could be combined, allowing the CRM application to be expanded to the server made available by the reconfiguration. By configuring both CRM servers within a single NetConnect application, users will be sent to “CRM 1” or “CRM 2” on a round robin basis.

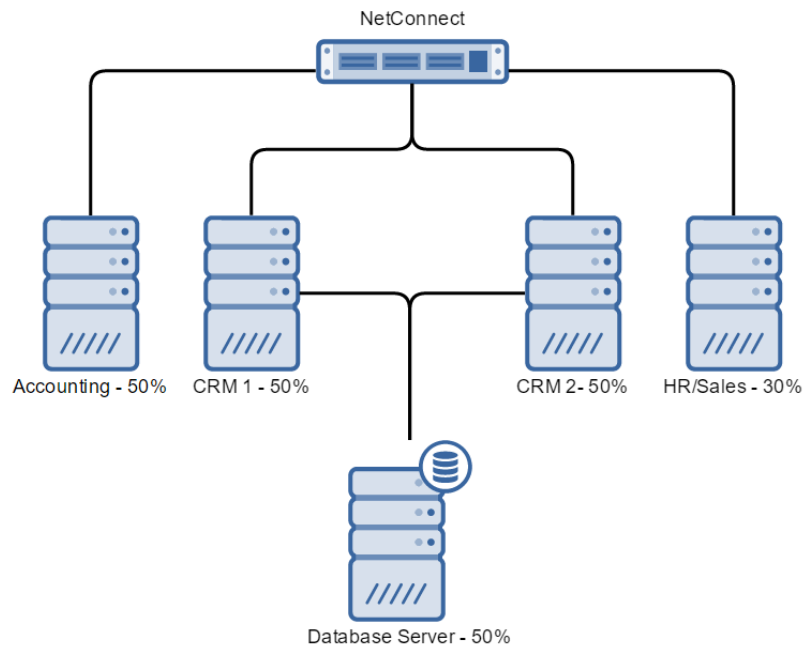


Fig.2

Configuration

Step 1 – Adding Application Servers to NetConnect

First, your application servers will need to be added into the list of available servers. For each server:

- Navigate to **Applications > Application Servers > Create New Server**.

- Enter each **Application Server Name**, **IP Address** and select **Enable RemoteApp Support**.

Step 2 – Configure the application

- Navigate to **Applications > Configuration**
- Highlight the application you wish to configure multiple server against and select **General Properties**. Note, the application you wish to publish servers to must be a 'Remote Application'.

Within the General Properties pages, tick the **Allocate Application Servers**. Note, HTML5 Client must be set to 'On'.

The screenshot shows the 'General Properties' configuration page for an application named 'Multiple Server'. The left sidebar contains a navigation menu with options like Home, Manage Access, Groups, Applications (selected), Configuration, Application Icons, Application Servers, Network Policies, Associate Access Level, Services, Reporting, Monitoring, Customization, System Configuration, and Authentication Settings. The main content area is titled 'Multiple Server' and contains the following fields:

- Application Name: Multiple Server
- Application Type: Remote Application
- Application Icon: rdpapp.gif (with a 'Browse...' button)
- Remote Application Type: ☒ Regular RDP, ☐ MyDesktop
- Full Address: (empty field) OR ☒ Allocate Application Servers ☐ User Select Address
- TS RemoteApp Support: Off
- Application Path: (empty field)
- Working Directory: (empty field)
- Color Depth: Device default
- Application Size: ☒ Full Screen, ☐ Workarea on Linux, Full screen on others, ☐ 640x480, ☐ 800x600, ☐ 1024x768, ☐ Custom
- Remote Protocol: RDP
- HTML5 Client: On

At the bottom, there are three buttons: 'Modify', 'Delete this app', and 'Make a Copy'.

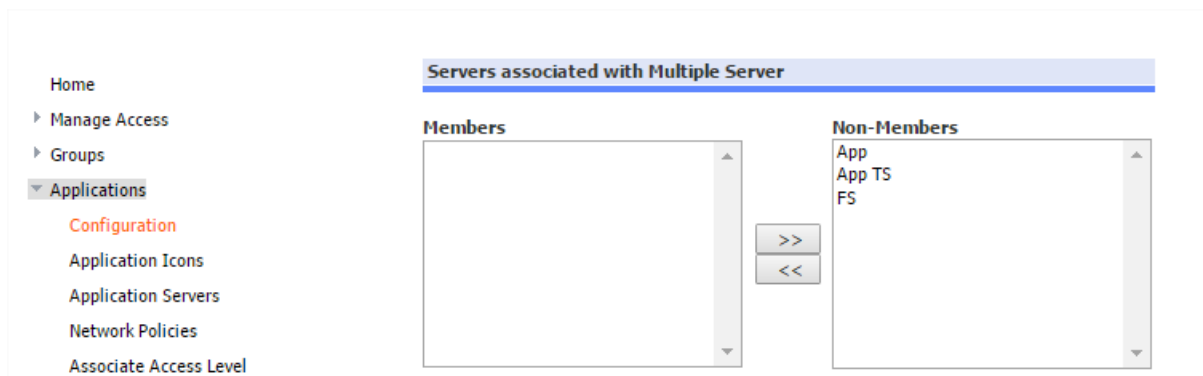
Step 3 – Assign Application Servers

- Navigate to **Applications > Configuration**.
- Highlight the application you wish to configure multiple server against and select **Application Servers**.

The screenshot shows the 'Applications' configuration page. The left sidebar is the same as in the previous screenshot, with 'Applications' selected. The main content area is titled 'Applications' and contains the following elements:

- A message: 'Select an Application and then click an Action below:'
- A list of applications: 'Multiple Server' (highlighted with a blue border).
- A list of actions:
 - >> Create New Application
 - >> General Properties
 - >> Authorized Users
 - >> Authorized Groups
 - >> Authorized Realms
 - >> Access Level
 - >> PF Rules
 - >> Password Forward
 - >> Application Servers

Finally, move the desired application servers from the Non-Members to the Members section, by selecting them in the non-members field, and selecting the '<<' icon.

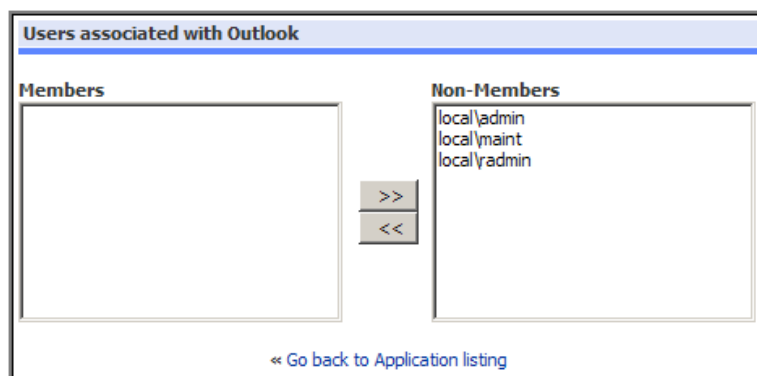


Application Management.

Authorising Access to Applications

Once an application is created, it must be assigned to specific users or groups. This section describes how to authorise user access to applications. Authorised applications appear on users' WebTop when they log in. Application access can be granted to individual users, a group of users or by V-Realm. This section describes how to grant access via the Applications menu.

- Navigate to **Applications > Configuration**. The Applications page opens.
- Select the name of the application that you wish to assign users to.
- Click one of the following options from the Actions menu.
 - **Authorised Users:** Assign application access to individual users. Note, the user must have logged into NetConnect prior to appearing.
 - **Authorised Groups:** Assign application access to groups of users. Note, a user from this group must have logged into NetConnect prior to a group appearing.
 - **Authorised V-Realms:** Assign application access to users of a particular V-Realm.
- Choose the user/group/V-Realm you want to grant access to this application from the Non-Members column, and then click the arrow to move them to the Members column.



Changes are saved automatically.

NOTE: You can use Control+Click to select multiple members, or Shift+Click to select a range of members.

Modifying an Existing Application

To modify an existing application:

- Navigate to **Applications > Configuration**
- Select the name of the application that you want to modify from the Applications list box and then click **General Properties**.

The General Properties page opens, allowing you to make the appropriate modifications. Once all changes are completed, click Modify. Note, if you do not click Modify your changes are lost. Please note that once an application has been modified, changes cannot be undone and as such must be re-adjusted manually if required. It is recommended that a configuration backup is taken as a roll back position before any changes are made to your NetConnect instance. Users will need to establish a new session to the modified application prior to any changes to take effect.

NOTE: Changes to authorised users and authorised servers take place immediately.

Deleting an Existing RDP Application

To delete an existing application:

- Navigate to **Applications > Configuration**.
- Select the name of the application that you want to modify from the Applications list box and then click **General Properties**.
- Click the '**Delete this app**' button located at the bottom of the General Properties page.

Please note that once an application has been deleted, it cannot be recovered. It is recommended that a configuration backup is taken as a roll back position before any changes are made to your NetConnect instance.

Make a Copy of an Application

NetConnect allows you to make a copy of any configured application, this function is useful for publishing multiple applications with similar attributes

To make a copy of an existing application:

- Navigate to **Applications > Configuration**.
- Select the name of the application that you want to copy from the Applications list box and then click **General Properties**.
- Click the '**Make a Copy**' button located at the bottom of the General Properties page.

V-Realm App allocation

As opposed to using a per user or per group system, applications can be published to V-Realms.

To allocate an application to a V-Realm:

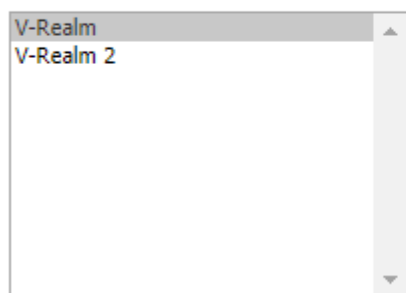
- Navigate to **Manage Access > V-Realms**.
- Select the V-Realm on the left hand side, then select **Get The User List**.

V-Realms



Select a V-Realm and then click an Action below:

V-Realms:



Actions:

- » Get The User List
- » Edit Realm Properties

- In the 'Applications Associated with V-Realm', moving a non-member application to the members list will grant all users within the V-Realm access to the application.
- Once in the Members List, Applications can also be a member in the '**Startup Items**' list. Members in this list will launch immediately after all authentication stages are complete for PC based sessions.

Applications Associated with 'V-Realm'

Members		Non-Members
Application 0 Startup Application 1	>> <<	Application 1 Application 2 Application 3 Application 4 Application 5 Application 6 Application 7 Application 8 Application 9 Application 10

Startup Items Associated with 'V-Realm'

Members		Non-Members
Startup Application 1	>> <<	Application 0

Chapter Four. System Administration.

This chapter provides an overview of the various tasks that should be considered before moving NetConnect into production, as well as an overview of typical tasks associated with system administration including.

- SSL Certificates.
- Licensing.
- Customisation.
- Reporting.
- Updating default passwords.
- Configuration backup and restore.
- Upgrading NetConnect.

4.1 Production Readiness

The following section provides an overview of some of the items to consider before deploying NetConnect to a production environment.

Assigning SSL Certificates

When installing and working on the NetConnect Environment, it is strongly recommended that an SSL Certificate is applied. An SSL certificate provides security when establishing an encrypted link with connections via NetConnect. The below guide will walk through the process of ordering and applying a certificate to your system. Please note that wildcard certificates are not supported.

This section describes how to install a certificate from a Certificate Authority (CA) and how to manage and store CA Signing Certificates (Root and Intermediate CA).

NOTE: It is assumed that the reader has some basic knowledge of public key infrastructure (PKI) and SSL.

Ordering the SSL Certificate

To begin ordering your SSL certificate, you will need to generate a new Certificate Signing Request (CSR) from your NetConnect instance; this is essentially a simple message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Please follow the below guide for ordering the certificate;

- Navigate to **System Configuration > General > SSL > Certs from CA > Request New Certificate**
- Complete the signing request form. Please note that:
 - The **Country Code** must be the recognised SSL two-digit code which corresponds to your location (specific codes can be found at <https://www.digicert.com/ssl-certificate-country-codes.htm>).
 - **State** must be three characters
 - **Common Name** should reflect the URL you are generating the certificate against.

New Certificate Signing Request (CSR) ?

Subject Information

Country:	AU
State:	NSW
Locality:	Artarmon
Organization:	northbridgesecure.com
Org. Unit:	
Common Name:	hostname.local ×
Email:	████@northbridgesecu

[Generate New Certificate](#)

IMPORTANT NOTE: Once the CSR has been generated, do not attempt to generate a new CSR or self-signed certificate as this will invalidate your request and void your certificate.

Once this field has been completed and you have generated a new certificate, you will need to copy the certificate that appears in the box below and navigate to your domain provider. Note, a matching private key is also generated and stored internally.

Subject Information:

Country:	AU
State:	NSW
Locality:	Artarmon
Organization:	northbridgesecure.com
Org. Unit:	
Common Name:	████northbridgesecure.com
Email:	████@northbridgesecure.com

Request Content:

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQIwgaAx CzAJBgNVBAYTAkFVMQwwCg'
ANOU1cxETAPBgNV
BAcMCEFydGFybW9uMR4wHAYDVQQKDBVub3J0aGJya
Y3VyZS5jb20xJDAi
BgNVBAMMG2tjb3BlLm5vcnRoYnJpZGdlc2VjdXJlLmNvb
CSqGSIb3DQEJ
ARYba2NvcGVAbm9ydGhicmlkZ2VzZWw1cmUuY29tMIIBIjANBgk
-----
  
```

- After verifying that all data is correct you can submit this CSR to a CA of your choice.
- Copy and save the Certificate Request to a text file. Make sure you include the full BEGIN and END lines and all of the dashes.
- Submit the new certificate request to your Certificate Authority.

Please note that it may take a short time for the CA Authority to generate and send the certificate once you have submitted the CSR. **In this time please do not generate another CSR** as this will generate a new internal private key and invalidate the original request.

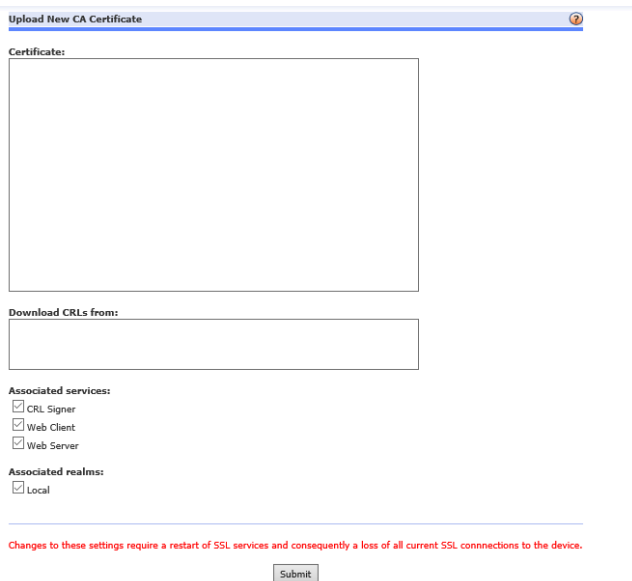
Once the CSR has been approved, your CA Authority will provide the required certificates via email or make them available on their portal for download

Installing the SSL Root and Intermediate Certificate

Installed CA server and client certificates must have the corresponding Root CA and any Intermediate Root CAs used in the issuing of the certificate present in the product's internal CA store.

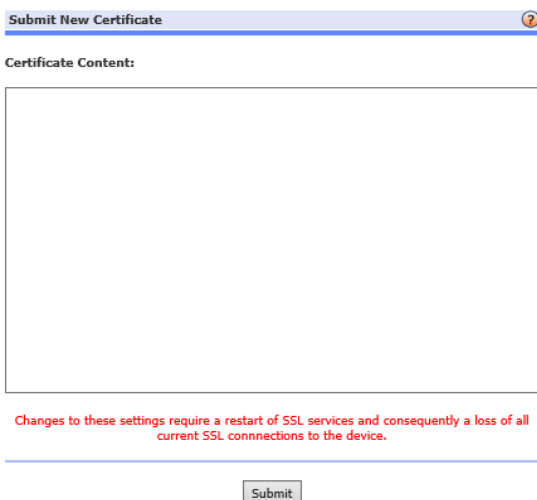
- 1) Navigate to **System Config > General > SSL > CA Certificate > Upload New**
- 2) Once here, you will need to paste the Root CA into the **certificate** field.
- 3) Ensure that all '**Associated Services**' and '**Associate Realms**' are selected.
- 4) Click '**Submit**'.
- 5) You will then be prompted to restart the SSL Service. This will result in a disconnection of any active connections to NetConnect.

Repeat this process for all Intermediate certificates provided by the CA Authority. All Intermediate Certificates must be uploaded separately



The screenshot shows the 'Upload New CA Certificate' interface. It features a large text area for the 'Certificate'. Below this is a 'Download CRLs from:' field. Under 'Associated services', the checkboxes for 'CRL Signer', 'Web Client', and 'Web Server' are all checked. Under 'Associated realms', the 'Local' checkbox is checked. A red warning message states: 'Changes to these settings require a restart of SSL services and consequently a loss of all current SSL connections to the device.' A 'Submit' button is located at the bottom right of the form.

- 6) Finally, you will need to navigate back to '**Upload Certs from CA**' and upload the **.crt** file. Navigate to **System Configuration > General > SSL > Certs from CA > Upload Cert from CA**



The screenshot shows the 'Submit New Certificate' interface. It features a large text area for 'Certificate Content'. A red warning message at the bottom states: 'Changes to these settings require a restart of SSL services and consequently a loss of all current SSL connections to the device.' A 'Submit' button is located at the bottom right of the form.

- 7) Once this has been uploaded, you will need to confirm that the settings are correct and select **'Set New Keys'**. Please note that at this stage, SSL services will restart, resulting in a disconnection of any active connections to NetConnect.

Set New Keys

Certificate Subject

Country:
State:
Locality:
Organization:
Org. Unit:
Common Name: kcope.northbridgesecure.com
Email:

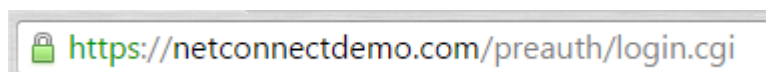
Certificate Issuer

Country: US
State:
Locality:
Organization: GeoTrust Inc.
Org. Unit:
Common Name: RapidSSL SHA256 CA
Email:

Changes to these settings require a restart of SSL services and consequently a loss of all current SSL connections to the device.

Set New Keys

- 8) Validate the process was successful by navigating to your NetConnect URL and confirm that the connection is secure.



Ensuring Date and Time are Configured Correctly

Occasionally when installing an SSL certificate it will not be accepted. The most common cause of this issue is when there is a time difference between NetConnect and the certificate information.

To ensure correct configuration, you will need to check the time on the environment.

- Navigate to **System Configuration > General > Date and Time**.
- Configure the time correctly so that it matches your local timezone.

Date & Time Configuration

Time Zone: Australia/Sydney

Date: Day: 12 Month: 05 Year: 2016

Time: Hour: 15 Min.: 56

Change

Note:
It is highly recommended that the system be restarted after this change in order to ensure that the change is applied to all existing processes.

Alternatively, you may opt to sync via NTP (Network Time Protocol).

- Navigate to **System Configuration > General > NTP**.
- Select the required server you wish to sync with and select the **'Sync'** button.

Network Changes

Once your NetConnect instance has been installed, configured and licenced there will be several steps you will need to take within your environment to ensure external access is available for all users. Specific steps will vary between environments and requirements, but in broad terms you will need to:

- **Assign a Public IP address.** This will be required in order to allow connections to NetConnect from outside of your network
- **Create a sub-domain.** This will be the URL that users will access your NetConnect instance from.
 - Note, you will need to ensure your DNS records are updated in order to resolve the sub-domain to your nominated Public IP address.
- **NAT IP Addresses.** Map the assigned Public IP address to your assigned internal IP address via Network Address Translation (NAT) within your router/firewall. This action will ensure traffic coming into your network on the nominated Private IP address is routed to your NetConnect instance.
- **Open Firewall Ports.** If accessing NetConnect from behind a firewall, port 80 (HTTP) and port 443 (SSL) must be open to allow traffic in both directions.

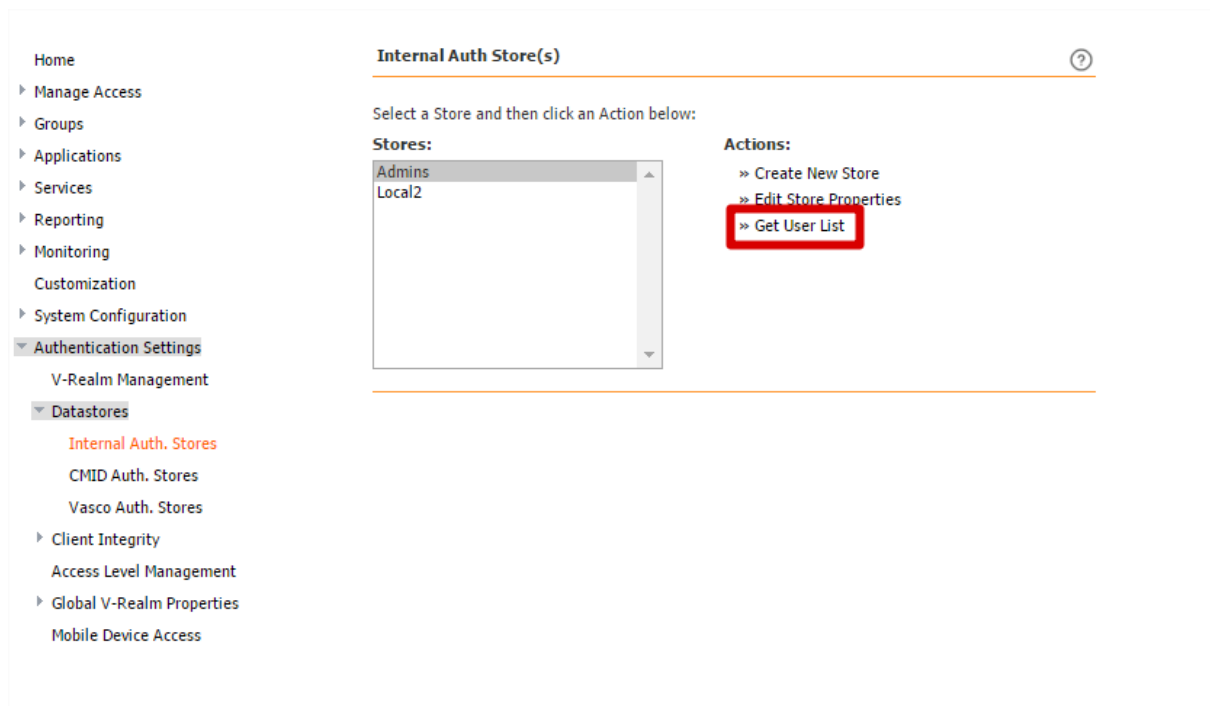
Changing an Administrator's Password

Prior to making NetConnect externally available, we strongly recommend you change the password of your administrator accounts:

- From the Administrator Site, navigate to **Authentication Settings > Datastores > Internal Auth Stores**

***WARNING:** If you change the password for the admin account, be sure to document the new password and keep it in a safe location. If you forget the password you will not be able to access NetConnect and there is no other way to gain access.*

- Select Admins and then click **Get User List** as shown.



- Select the admin account for which you want to change the password and then click **Edit Properties**.

The following example uses the radmin account.

Store Name: Admins

Select a User and then click an Action below:

Users:

admin
maint
radmin

Actions:

» [Edit Properties](#)

- Enter a new password for this administration account

Properties for user: radmin

Change Password

New Password:

New Password Confirm:

Update Password

The Password field is case sensitive. The password may have any alphanumeric character, or punctuation marks such as the following English punctuation marks:

!"#\$%&'()*~^|\`@{[+;*:]<,>./_ \ .

- Enter a new password in the New Password field and then type the identical password in the New Password Confirm field.
- Click Update Password to save the changes.

If you changed the password, log out and then log in again using the new password.

Licensing

NetConnect must be appropriately licenced to allow access to non-admin accounts. This section describes how to install the product licence to enable user access to the configured features and services. To complete this process, you will need the licence key from your integrator or distributor. The licence key will reflect the user count and expiration date in accordance with your current support contract.

To install the product licence, do the following.

- From the Administrator Site, click System Configuration, and then click Licensing.

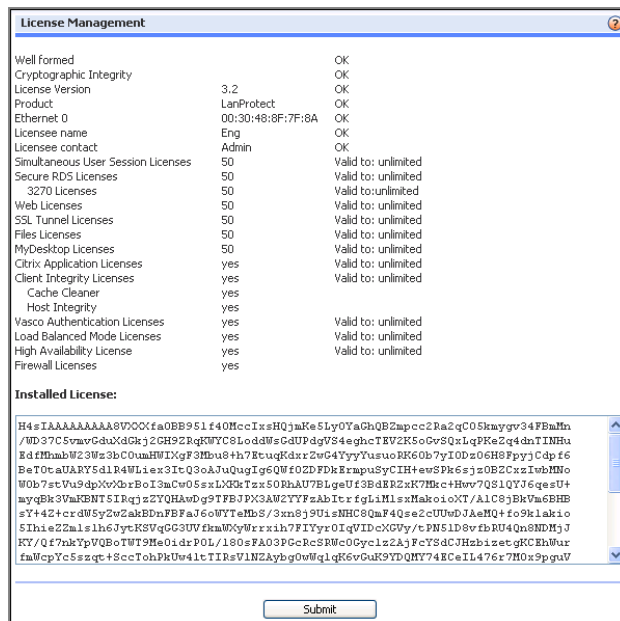
▼ **System Configuration**

- Network
- Load Balancer Configuration
- General
- ▼ **Licensing**
 - Reset

The Licence Management page appears.

- Copy the encoded text and paste it in the text box labelled Installed Licence.

- Click Submit. The Licence Management page with an installed licence is shown.

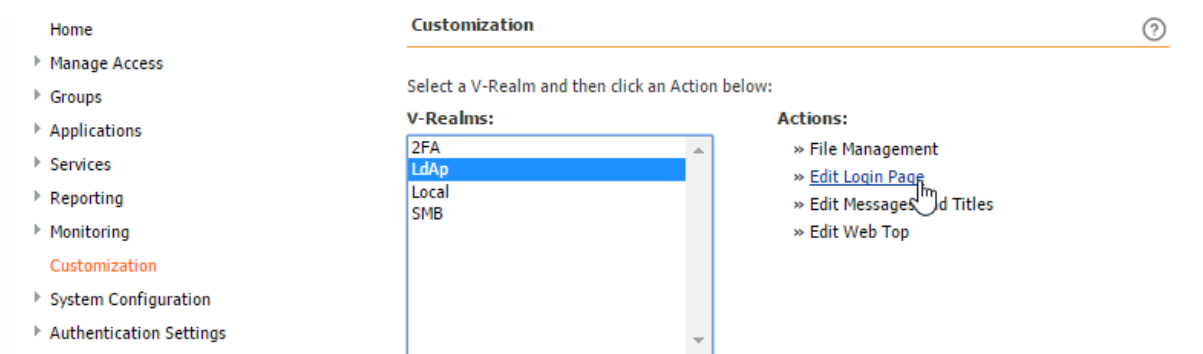


Customisation

Edit Company Name and Logo on Login Page

This section describes how to change the company name and logo that appears on the login page.

- From the main menu, navigate to **Customisation**.
- Select the name of the V-Realm with log in page you want to customise and then click **Edit Login Page**.



NOTE: The login page that appears for users to enter their credentials is the one associated with the V-Realm listed first under Authentication Settings>V-Realm Management.

The Customisation Login page appears

Customization::Login

Login Page:

Login Page Title:

Company Name:

Logo Link:

Logo Image:

Click here to select custom logo.

[Preview](#)

[« Back to Realm List](#)

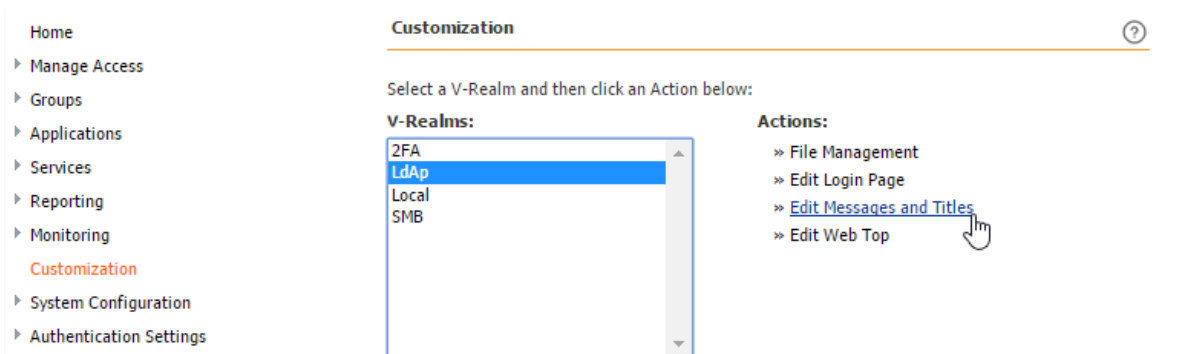
- **Login Page.** Leave the default setting as 'Standard'.
- **Login Page Title.** Enter a name for the login page. By default this is set to "login".
- **Company Name.** Type a name in the Company Name field.
- **Logo Image.** Browse to a logo of your choice using the browse button.
 - The logo must be in the form of gif, jpeg, or png.
- Click **Update** to complete.

Creating Custom Messages

You can customise all of the possible messages a user can see on the log in page. You can customise the information and error messages that users see on the login page. There are a total of 27 messages that can be customised, including four customisable titles. These titles are User name, Password, V-Realm, and the text displayed on the Log-in button.

To create custom messages:

- From the main menu, select **Customisation**.
- From the Customisation page, select the name of the V-Realm for which you want to customise messages and then click **Edit Messages and Titles**



The Edit Messages and Titles page opens.

- Enter your custom messages as needed. Note that HTML tags are permitted with your custom text.
- After you've made all of the changes, scroll to the bottom of the page and click Submit Changes. Users will now see the custom messages and titles.
- To revert back to the default messages, click Set All Default Values located on the top of the page.

Customising Application Icons

When you create an application, whether it's a Secure RDS, Web, or Tunnel application type, you assign an icon to graphically represent the application on the end user's WebTop. By default, a set of standard icons is provided. However, you can also install additional icons as needed.

NOTE: Icons should be 35 x 35 pixels in size and 8 bits per pixel (256 colours) for depth.

To install icons, you must upload an image of the icon in gif or jpg format via the Application Icons tool. This section describes how this is done.

Uploading Icons

To upload gif files:

- Navigate to **Applications > Application Icons**.
- Click **Browse**, and locate the icon you want to upload.
- Once located, click **Upload**. The icon now appears on the list of available icons for publishing applications.

The screenshot shows a web application interface for managing application icons. On the left is a navigation menu with options: Home, Manage Access, Groups, Applications (selected), Configuration, Application Icons (highlighted with a mouse cursor), Application Services, Network Policies, Associate Access Level, Services, Reporting, Monitoring, Customization, System Configuration, and Authentication Settings. The main content area is titled 'Application Icons' and includes a help icon. Below the title, a text block explains that users can upload and delete their own icons, with a note about the 35x35 pixel size requirement. An 'Upload an Icon' section contains a 'Choose File' button (showing 'No file chosen') and an 'Upload' button. Below this is a table titled 'List of Current Custom Icons' containing five entries, each with a thumbnail icon, a filename, and a 'Delete' button.

List of Current Custom Icons		
	Accounting.gif	<input type="checkbox"/> Delete
	Accounting_HTML5.gif	<input type="checkbox"/> Delete
	Admin_HTML5.gif	<input type="checkbox"/> Delete
	Adobe-Acrobat-Reader.gif	<input type="checkbox"/> Delete
	Adobe-Acrobat-Reader_HTML5.gif	<input type="checkbox"/> Delete

4.2 System Administration

Configuring General Settings

The General Settings page, is used to configure the general network information, including setting the Host name of the box, the Primary and Secondary DNS, the Default Gateway and the Ethernet interfaces.

To configure the General Network information, navigate to **System Configuration > Network > General**

Home

Manage Access

Groups

Applications

Services

Reporting

Monitoring

Customization

System Configuration

Network

General

Hosts File

IP Forwarding and NAT

Routing

Firewall

Troubleshooting

Load Balancer Configuration

General

Licensing

Software Upgrade

High Availability

Monitor Configuration

Shutdown

Authentication Settings

General Network Information

Host Name:

nsslab.northbridgesecure.com

Eth0 Interface

IP Address:

10.2

Subnet Mask:

255.

MAC Address:

00:0C:

Eth1 Interface

IP Address:

203.

Subnet Mask:

255.

MAC Address:

00:0C

Default Gateway:

203.

Primary DNS:

10.

Secondary DNS:

8.

Enable DNS Cache:

Off

DNS Suffixes

Add DNS suffix:

Add

DNS Suffixes:

northbridgesecure.com

Delete selected

Submit

- **Host Name.** The host name must match the common name on the digital certificate installed on the product. Whenever you change the host name, ensure you also have a matching digital certificate to install. If the digital certificate and the hostname of the product do not match, the end-user receives an error. The host name should also be in the global DNS and resolve to an IP address on the firewall.
- **Eth0 Interface.** The IP address and subnet mask of the primary Ethernet interface. Note that the MAC address of this interface is displayed.
- **Eth1 Interface (optional).** The IP address and subnet mask of the secondary Ethernet interface. Leave these fields blank if you are not configuring a secondary Ethernet interface.
- **Default Gateway.** This is usually the address of the router that is used to reach the Internet.
- **Primary and Secondary DNS.** Enter the IP address of your DNS servers.

DNS Caching

If publishing an application via a hostname, DNS Cache will need to be 'Off'. In order to configure DNS Cache:

- Navigate to **System Configuration > Network > General**
- Set **Enable DNS Cache** to 'Off'.

DNS Suffix

If you are using NetConnect to connect to any domain resources via hostname, it is recommended that the domain is added to the DNS Suffix list; this will simplify configuration and end user access. By defining a global list of possible suffixes, attempts are made to resolve unqualified queries using each entry in the search list in turn until a match is found.

To add a DNS Suffix:

- Navigate to **System Configuration > Network > General**
- **Add DNS Suffix.** Type in the DNS suffix and click.

The entry will now appear within the DNS Suffixes list. Note, individual entries can be deleted by highlighting the specific entry and clicking **Delete Selected**.

Home

- Manage Access
- Groups
- Applications
- Services
- Reporting
- Monitoring
- Customization
- System Configuration**
 - Network**
 - General
 - Hosts File
 - IP Forwarding and NAT
 - Routing
 - Firewall
 - Troubleshooting
- Load Balancer Configuration
- General
- Licensing
- Software Upgrade
- High Availability
- Monitor Configuration
- Shutdown
- Authentication Settings

General Network Information

Host Name:

Eth0 Interface

IP Address:

Subnet Mask:

MAC Address:

Eth1 Interface

IP Address:

Subnet Mask:

MAC Address:

Default Gateway:

Primary DNS:

Secondary DNS:

Enable DNS Cache:

DNS Suffixes

Add DNS suffix:

DNS Suffixes:

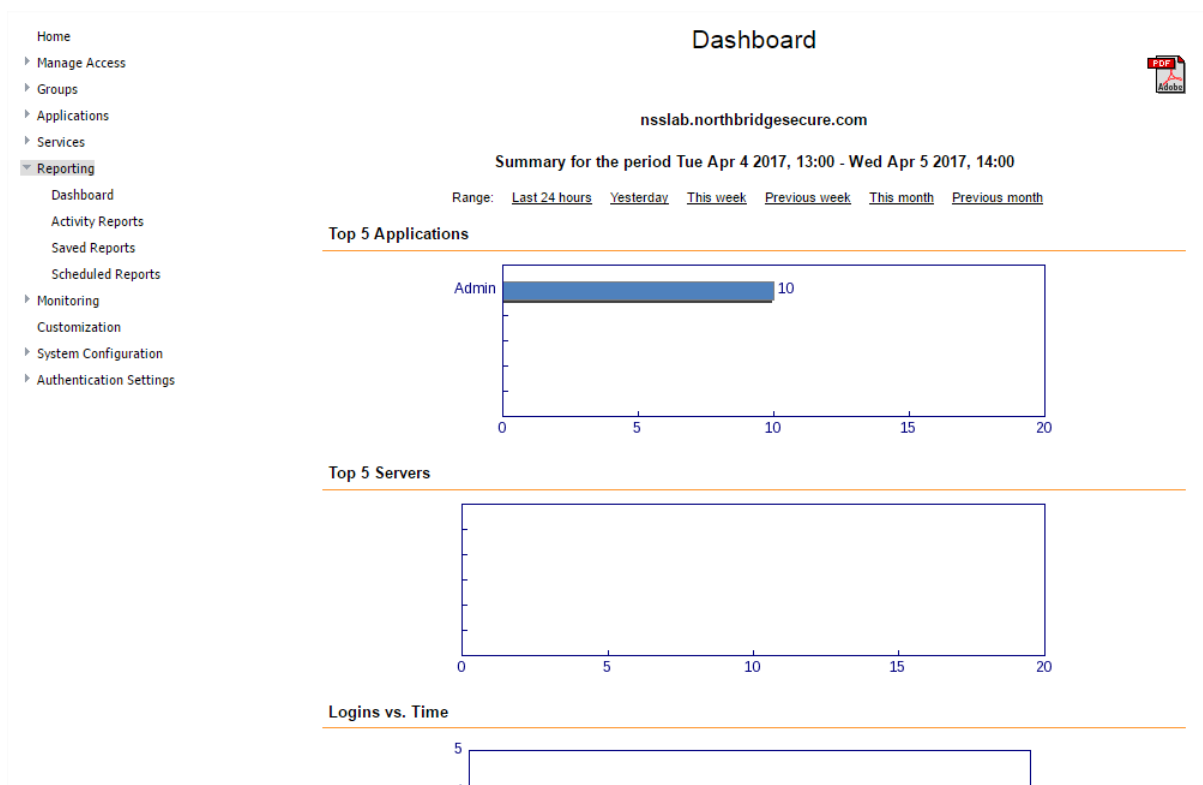
Reporting

This section describes how to set up and use the reporting features. The following topics are discussed.

- Reporting Dashboard
- User Activity Reports
- Saving Reports

Reporting Dashboard

The dashboard provides an overview of the product traffic.



User Activity Reports

Within the Activity Reports section, you are able to:

- Creating an Activity Report
- Filtering and Sorting Options
- Activity Report Example

Creating an Activity Report

To create a detailed activity report, do the following.

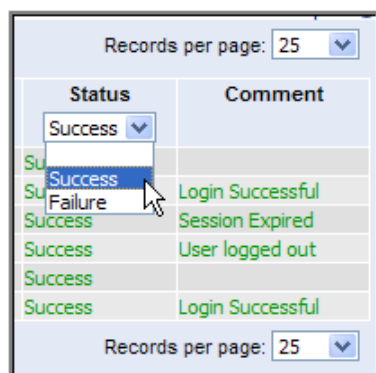
- From the Administrative Site, click **Reporting**.
- Select **Activity Reports**.

A list of activities that have occurred is displayed as shown.

Activity Reports									
<div> Home Manage Access Groups Applications Services Reporting Dashboard Activity Reports Saved Reports Scheduled Reports Monitoring Customization System Configuration Authentication Settings </div>									
<div> <div> First Prev Next Last </div> <div> Apr 05 2017 12:49 </div> <div> Apply Filter Reset Filter </div> <div> Export </div> </div>									
Date	Realm	Username	Action	Source	Destination	Application	Status	Comment	
Apr 5 12:49:05	Idap	jp	Logout	10			Success	User Logged Out	
Apr 5 12:49:03	Idap	jp	Login	10			Success	Login Successful	
Apr 5 11:43:23	Idap	jp	Logout	10			Success	Session Expired	
Apr 5 11:41:07	Idap	jp	Application Terminated	10		Admin	Success		
Apr 5 11:28:49	Idap	jp	Application Started	10		Admin	Success		
Apr 5 11:28:47	Idap	jp	Login	10			Success	Login Successful	
Apr 5 11:28:47	Idap	jp	Logout	10			Success	Logged In From Another Terminal	
Apr 5 11:14:22	Idap	jn	Application Started	10		Admin	Success		
Apr 5 11:14:20	Idap	jn	Login	10			Success	Login Successful	
Apr 5 10:38:46	Idap	jn	Application Terminated	10		Admin	Success		
Apr 4 20:23:49	Idap	jn	Logout	10			Success	Session Expired	
Apr 4 20:23:49	Idap	jn	Application Terminated	10		Admin	Success	User logged out	

Filtering and Sorting Options

The following sort and filter options are available:

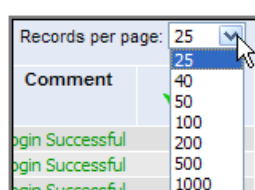


Sorting by Action or Status

Use the Action and Status drop down list boxes to further narrow results. For instance, to view only “successful” connections, select Success from the Status list box.

Changing Number of Records Displayed Per Page

By default, ten records per page are displayed. To change the number of records shown on a single page, select the desired number from the drop down list box and then click Apply Filter.



Clearing Sort Criteria

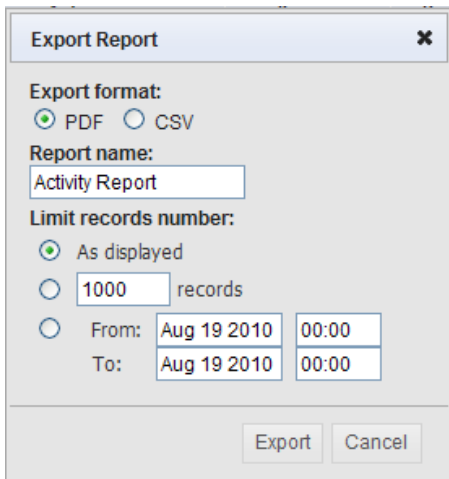
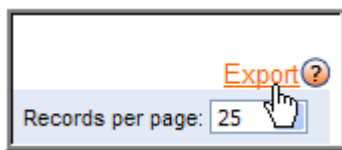
To reset and clear the filtering fields, click the Reset Filter button



Saving Reports

Reports can be saved in CSV format, follow these steps:

- From the Administrative Site, click **Reporting > Activity Reports**.
- Use the search fields to create the desired report content.
- Click **Export**.



- Specify the following:
 - **Export Format:** Choose CSV.
 - **Report Name:** Type a name for this report.
 - **Limit records number:** Choose 'As displayed' to include all records shown in the report, or type the number of records you would like saved, or choose the interval of time for which records will be included in the report.
- Click **Export**. A success message appears.
- To view or download to report navigate to **Reporting > Saved Reports**.

Backing up and Restoring NetConnect Configuration

The Backup/Restore feature allows you to save the current configuration settings and restore those settings at a future time. Configuration settings such as applications, application servers, user accounts and permissions, product licence, and your customised GUI and logos can be safely backed-up and later restored. We recommend a backup of the configuration settings are taken after each system change.

Changes to the configuration cannot be made while a backup is in progress. Logging in is also prevented until the backup process is complete.


Manually Creating a Backup File

To back up current settings manually, do the following:

- From the Administrator Site, click System Configuration and then click Backup/Restore, as shown below:



A screenshot of the 'Backup/Restore' configuration page. The page has a title bar 'Backup/Restore' with a help icon. It contains two main sections: 'Backup' and 'Restore'. The 'Backup' section has a 'Backup' button. The 'Restore' section has a text area for the backup file name, a 'Browse...' button, and a 'Restore' button. Below these sections is a table titled 'List of backup files currently stored on this unit:'.

	Backup date:	Backup size:
	Mon Aug 24 13:44:41 2009	2,732,042
		Total size: 2,732,042

- Click Backup. The backup process begins.
- Click Back to download the file.

A screenshot of the 'Backup/Restore' page showing a message: 'The backup process has been started. The backup file will be available to download once the process is complete.' Below the message is a 'Back' link with a mouse cursor pointing to it.

- To download the file, click the floppy disk icon.

Backup/Restore

Backup: Creates a backup of the system configuration for this Netilla unit.

Restore: Restores this Netilla unit to a prior configuration. Use Browse to locate the file or type the name of the back up file (browser permitting). Please enter the name of the backup file to upload to this box and restore from.

List of backup files currently stored on this unit:

	Backup date:	Backup size:
	Mon Aug 24 13:44:41 2009	2,732,042
	Mon Aug 24 13:47:50 2009	2,732,042
Total size:		5,464,084

- You are prompted to open or save the file. Click Save. This completes the Backup procedure.

Using the Restore Feature

To restore the configuration settings file that you have previously backed up, do the following.

- From the Administrator Site, click System Configuration and then click Backup/Restore.
- Click Browse to locate your previously created backup file. Select that file and then click Open. The file is displayed in the Restore text box.
- Verify the file path and name and click Restore. The Restore process begins and is usually complete within five minutes. However, this process may take longer depending on the size of the data store. When complete, you are presented with a Restore Complete message.
- Log out completely.
- Log back in to verify your restored changes.

Upgrading NetConnect.

Periodic updates will be made available to supported customers in order to provide new features, modifications and bug fixes. This section provides a broad overview of the software upgrade process.

Upgrading from a pre-Release 8 instance.

Several non-core features within NetConnect are currently only functional under certain scenarios due to changes from external parties on which they rely. This includes:

- Web File Bookmarks.
- Web via Reverse Proxy.
- Idle timeout.
- Cache Cleaner.
- Pop-up Unblocker.
- Citrix Application Set.
- Citrix Point Application.
- Client Integrity.

Especially affected are those features that rely on the Java Port Forwarder. Support for these features will be on a reasonable efforts basis with release 8.3. As a result, Northbridge Secure cannot guarantee that these feature will function in the same fashion as previous releases and recommend that

appropriate testing is undertaken before upgrading any environments which depend on these elements of NetConnect. Please contact the Customer Support team for any required clarifications.

Best Practice – Physical

When upgrading your NetConnect appliance, consider the following:

Install the virtual edition with the same version as the appliance, and import your most recent backup. It is important that after every stage you take a snapshot and a configuration backup. Use the virtual edition to upgrade to the desired version (recommended to use the latest), and as before take a snapshot and configuration backup.

Install a fresh image of the desired version on the appliance and restore the backup taken from the virtual edition.

optional

Before you upgrade the Physical appliance, swap the IP addresses of the editions around so that you may test to check whether if the configuration was corrupted during the upgrade process, and that all functionality still works (this step is optional, as it requires a new licence for the virtual environment to log users in and test functionality. As this licence comes from Northbridge Secure, there may be extra time added to your upgrade as you wait for a licence to be issued).

Best Practice – Virtual

When upgrading your NetConnect appliance, consider the following:

Install a second virtual edition with the same version as your current virtual, and import your most recent backup. It is important that after every stage you take a snapshot and a configuration backup. Use the second virtual edition to upgrade to the desired version (recommended to use the latest), and as before take a snapshot and configuration backup.

Install a fresh image of the desired version on the first virtual edition and restore the backup taken above.

optional

Before you upgrade the first virtual edition, swap the IP addresses of the editions around so that you may test to check whether if the configuration was corrupted during the upgrade process, and that all functionality still works (this step is optional, as it requires a new licence for the virtual environment to log users in and test functionality. As this licence comes from Northbridge Secure, there may be extra time added to your upgrade as you wait for a licence to be issued).

Upgrade from 8.1.x.to 8.3.0

If you wish to upgrade from a version older than 8.1, a fresh instance of NetConnect will be required. Please refer to the current 'NetConnect Upgrade Path' document for further details.

1. Download the Upgrade-8.1.0.0-8.3.0.1 file
2. Navigate to **System Configuration > Software Upgrade** and apply the patch
3. Reboot your NetConnect instance
4. Take backup of the 8.3.0 configuration and store off the appliance

Once the reboot has completed, your NetConnect instance will be running the latest NetConnect version.

Shutdown and Restart.

You can use the Shutdown option from the System Configuration menu to either shutdown or restart NetConnect.

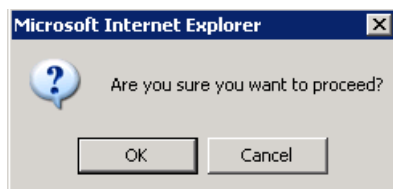
- **Reboot:** Restarts NetConnect.
- **Shutdown:** Shut down turns the power to the product off.

To reboot or shutdown NetConnect, do the following.

- From the Administrator Site, click System Configuration and then click Shutdown from the submenu.



- Select the preferred action. A confirmation message appears.



- Click OK to proceed. When Reboot is selected, the following message appears.

The system is rebooting.

If you selected Shutdown, the following message appears

The system is shutting down. Please allow a minute or two to complete, then turn the power off.

You will see an Access Denied message while the system reboots and after it shuts down.

- If you chose restart, you are prompted to “Enter decryption password”. Type the admin password and then press Enter. The boot process continues. Once the restart is complete you will see the log in page.