BlackShield ID Best Practice

Implementation Guide for a Complex Network

Document Scope

This document is designed to demonstrate best practice when implementing and rolling out a two-factor authentication strategy. Working from an example complex case study scenario, this guide will show how we can help you overcome some of the biggest issues you would face when moving from a static password policy to two-factor authentication (2FA):

- Migrating users from static passwords to token authentication in an orderly and controlled process
- Minimising the demands on IT staff during the token issuing process
- Achieving all this transparently and with little to no impact on users and Security Administrators

In addition to that, through this guide you will gain an in-depth knowledge of how BlackShield ID works, how easily it integrates within your existing systems and be able to see how little management it requires once it's running. If you would like to see the full guide on BlackShield ID features and functionalities, we will be happy to provide you with our comprehensive BlackShield ID Pro Administrator Guide.

If at any time you would like to speak to one of our team, please get in touch:

t: +1 800 30707042
e: support@cryptocard.com

Content Overview

1. MyCo Case Study Scenario

Current Infrastructure:

- There are 1,500 users accessing the network via three main routes:
  i) 500 users access the network internally
  ii) 900 users access the network both locally from the office and remotely via a combination of Cisco VPN, Outlook Web Access (OWA, 2003) and Citrix Web Interface 4.6
  iii) 100 external contractors and suppliers access the network via Citrix

- MyCo will soon be extending Citrix Web Interface Access to another 100 users

- All users have static usernames and passwords for network logins

- Active Directory is the user account repository and users are grouped as below:

500 users	Office staff
250 users	R&D
225 users	Sales
225 users	Marketing
200 users	IT
100 users	Citrix Access only
100 users	Contractors and suppliers

2FA Implementation Goals:

- Over a three week period, deploy a combination of SMS zero-footprint tokens, software (MP) tokens and KT keychain hardware tokens with low impact on Security Administrator time commitments.

- Issue tokens to 900 employees for remote network access while still allowing static password access from within the office only.

- 500 office-based employees will not have tokens at this time and will continue using static password access but from within the office only.

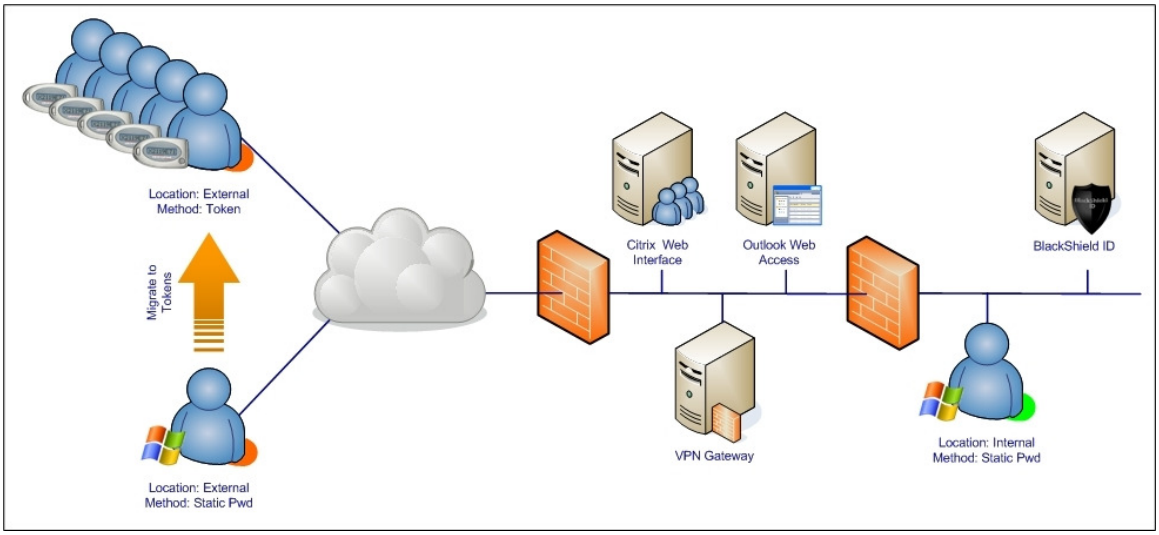
- Issue tokens to 100 contractors and suppliers for remote access via Citrix only and allow authentication only with a token.

- During token provisioning process, all users will still be able to access the network with their static passwords.

- Once tokens for remote access only users have been provisioned, static passwords will only be allowed for a certain amount of time before they are deactivated.

- Business continuity and pandemic planning measures must be in place to issue SMS tokens at a 'flip of a switch' to the 500 Office staff group to allow remote access via VPN only in case of emergency.

Target Infrastructure Model:



Additional Items

I. Minimising administrator time commitments to provisioning users with tokens.
In order to minimise administrators' time commitments, MyCo will be utilising a number of BlackShield ID capabilities that reduce the provisioning effort to nearly zero:

- Import of Pre-Initialised Tokens
  Eliminating local token initialisation, this feature allows tokens to be purchased in batches and imported into the server as required. As CRYPTOCard tokens do not expire, the useful life of the token in the field is not shortened by the amount of time it is kept in inventory.

- Rule-Based Provisioning
  Removing the need for a Security Administrator to be involved in the provisioning and deployment process, this feature will be configured to automatically assign tokens and initiate provisioning and self-enrollment whenever users are added to the designated LDAP groups. This helps facilitate a scheduled and controlled migration away from static passwords.

- Threshold Alerts
  This feature will automatically alert the Security Officer in the event that a user does not complete the enrollment process within the enrollment and migration periods.

- Pre-Auth Rules
  A completely transparent, controlled migration can be achieved by configuring a few simple rules within BlackShield, allowing it to distinguish between remote users: those that should only be able to access Citrix and those that should only be able to access OWA and the network via VPN.

  In addition, Pre-Auth rules will be configured to allow remote access using static passwords until the rule expires or the user completes self-enrollment of a token.

  Finally, Pre-Auth rules will be configured for specific access rights, such as any account that is locked or suspended in LDAP is automatically respected by BlackShield ID. If a user attempts to authenticate outside of time/day restrictions set in Active Directory, the authentication request will be rejected by BlackShield ID.

II. Maximising the seamlessness and simplicity of the user migration experience.
To achieve high user acceptance when implementing any process change planning, testing and communication are vital. In this case study we'll use a number of features in BlackShield ID to:

- Test the provisioning plan, end-user instructions, communications and overall login experience before rolling the solution out to the entire user community.

- Customise notification and enrollment messaging for effectiveness with our user population. We'll also add branding to these messages.

- Configure threshold alerts so that the help-desk can effectively and efficiently resolve any end-user authentication queries.

III. The remainder of this document describes the configuration and testing of a BlackShield ID implementation in MyCo that achieves the security, migration, transparency and administrative goals.

The references to networking and productivity products such as Citrix, Microsoft OWA and Cisco ASA are primarily to add clarity and provide examples of what can be accomplished with BlackShield ID.

The principles, steps and configurations can be easily applied to more complex networks, and applications supporting a much broader range of 3rd party products.

2. Initial Steps

Before implementation, some initial steps need to be identified in preparation for the BlackShield ID installation and set up. These are detailed below:

Creating Rule Based Provisioning Policies

MyCo will need to create three token provisioning rules as a combination of keychain (KT) hardware, MP (Software token), and SMS zero footprint tokens will be used.

i. Rule name: Keychain token users
- Token type: KT
- Auto revoke: enabled
- AD Group: Crypto KT

ii. Rule name: MP token users
- Token type: MP
- Auto remove: enabled
- AD Group: Crypto MP

iii. Rule name: SMS token users
- Token type: SMS
- Auto revoke: enabled
- AD group: Crypto SMS

Creating Pre-Authentication Rules
* remove the Allow All rule first

i. Self-enrollment rule
- Filter: LDAP Pass-through, when user has no BSID token / password, forward to LDAP; if LDAP fails, forward back to BlackShield
- Agent is Token Validator
- User is member of: Sales, IT, Contractors, Marketing, R&D, Citrix Only
- User is not externally locked / disabled / restricted

Tip: *Office group is not needed as SMS tokens do not go through self-enrollment.*

ii. Citrix access rule with LDAP authentication
- Filter: LDAP pass-through, when user has no BSID token / password, forward to LDAP; if LDAP fails reject the authentication
- Agent is Citrix
- Date is or after YYYYMMDD and is before YYYYMMDD
- User is a member of: Citrix only, IT, Sales, Marketing, R&D
- User is not externally locked / disabled / restricted

Tip: *The Office group is not added to this rule as they are only allowed access via VPN. The Contractors group is also not added to this rule as it would allow them access with LDAP credentials.*

iii. Cisco VPN rule with LDAP authentication

- Filter: LDAP pass-through, when user has no BSID token / password, forward to LDAP; if LDAP fails reject the authentication
- Agent is IAS
- Date is or after YYYYMMDD and is before YYYYMMDD
- User is a member of: IT, Sales, Marketing, R&D
- User is not externally locked / disabled, restricted

Tip: *The Office group is not added to this rule as they are only allowed access via VPN and only with a token. The Citrix only group and Contractors group are also not added to this rule as it would allow them access with LDAP credentials or tokens.*

iv. OWA rule with LDAP authentication

- Filter: LDAP pass-through, when user has no BSID token / password, forward to LDAP; if LDAP fails reject the authentication
- Agent is IIS
- Date is or after YYYYMMDD and is before YYYYMMDD
- User is a member of: IT, Sales, Marketing, R&D
- User is not externally locked / disabled / restricted

Tip: *The Office group is not added to this rule as they are only allowed access via VPN The Citrix only group and Contractors group are not added to this rule as it would allow them access with LDAP credentials or tokens.*

v. Citrix contractor rule

- Agent is Citrix
- User is a member of Contractors

Tip: *This rule allows access for only the users in the Contractors group via Citrix and only with a token.*

vi. Citrix access rule token authentication only

Agent is Citrix
Date is or after YYYYMMDD
User is a member of Citrix only, IT, Sales, Marketing, R&D
User is not externally locked, disabled, restricted

Tip: *The Office group is not added to this rule as they are only allowed access via VPN.*

vii. Cisco VPN rule token authentication only

- Agent is IAS
- Date is or after YYYYMMDD
- User is a member of IT, Sales, Marketing, R&D
- User is not externally locked, disabled, restricted

Tip: *The Office group is not added to this rule at this time as they are only allowed access via VPN when MyCo is required to implement their emergency business continuity plan.*

viii. OWA rule token authentication only

- Agent is IIS
- Date is or after YYYYMMDD
- User is a member of IT, Sales, Marketing, R&D
- User is not externally locked, disabled, restricted

Tip: *The Office group is not added to this rule as they are only allowed access via VPN.*

Prerequisites Prior to BlackShield ID Setup

The following are required to be configured and have users successfully authenticating with static passwords prior to the set up of BlackShield ID:

- Cisco VPN
- OWA Exchange 2003 form based login
- Citrix Web Interface 4.6

3. Implementation Plan Overview

The plan is as follows:

I. Install and configure BlackShield ID Pro
   a. Install BlackShield ID
   b. Configure BlackShield SMS settings, Email settings, and Events and Alerts
   c. Create Pre-Authentication rules and Rule Based Provisioning
   d. Importing of pre-initialized tokens

II. Test token provisioning. Configure and test 2FA in a development / test environment. Prepare instructions to communicate changes to end-user community.

III. Install BlackShield ID NPS IAS Agent
   a. Configure IAS to accept RADIUS authentication from: *(See NPS IAS Documentation)*
      - VPN (Cisco Concentrator) and local host *(RADIUS authentication test)*
   b. Test RADIUS authentication via NTRadPing tool against IAS *(Test with LDAP pass through)*

IV. Install BlackShield ID IIS6 Agent
   a. Configure IIS 6 Agent to protect OWA forms based login *(See IIS 6 Documentation)*
   b. Test OWA forms based login *(Test with LDAP pass through)*
   c. Configure IP Exclusion List *(Test internally with normal credentials)*

V. Install BlackShield ID Citrix Web Interface 4.6 Agent
   a. Test Citrix Web Interface 4.6 *(Test Externally with LDAP pass through)*
   b. Configure IP Exclusion List *(Test internally with normal credentials)*

VI. Configure VPN to authenticate against BlackShield ID
   a. Test RADIUS authentication via Cisco Concentrator *(Test with LDAP pass through)*

VII. Use Rule-Based Provisioning and commence token roll out

VIII. Test all remote access that has been changed over to use 2FA

4. BlackShield ID Pro: Installing & Configuring

Installing

There are some prerequisite system requirements that must be in place prior to installing BlackShield ID Pro:

- Microsoft IIS 6 or IIS 7
- .NET Framework 2.0
- .NET 2.0 Web Extension Enabled within IIS 6
- Application Development role enabled within IIS 7
- MSXML 6.0 SP1
- IAS (Windows 2003 Server) or NPS (Windows 2008 Server) for RADIUS authentication

For full system requirements, please refer to the 'Getting Started' section of the BlackShield ID Pro Administrator Guide.

Note: *The default database that comes pre-packaged with BlackShield ID Pro is PostgreSQL. If you wish to use a supported external database (MySQL, MSSQL, Oracle) select the option for a Custom setup during the BlackShield ID installation process and deselect the PostgreSQL option.*

Configuration

After installation, log into the BlackShield ID Manager using a Microsoft Administrator username and password. Once logged in, the web browser will redirect to the System Admin page. The system requires the SQL Source (database location), Licensing and User Source (User locations) to be configured before access to the rest of the BlackShield ID system is granted.

Note: *If PostgreSQL was installed during the installation of BlackShield ID then you can skip the configuration of the SQL Source as it will already be pre-configured after log on.*

After access is given, the following should also be configured from the System Admin page:

- Add SMTP Server settings under Mail Settings Section and test the settings
- Add an Administrative Email Address or Email distribution list to the Events and Alerts Section
- Modify Base URL under Self-Enrollment so it can be accessed by all users
  (If https is not to be used, remove the ‘s’ from https in the self-enrollment base URL and remove the self-enrollment over SSL checkmark.)
- Configure SMS Settings for BlackShield ID and test the settings

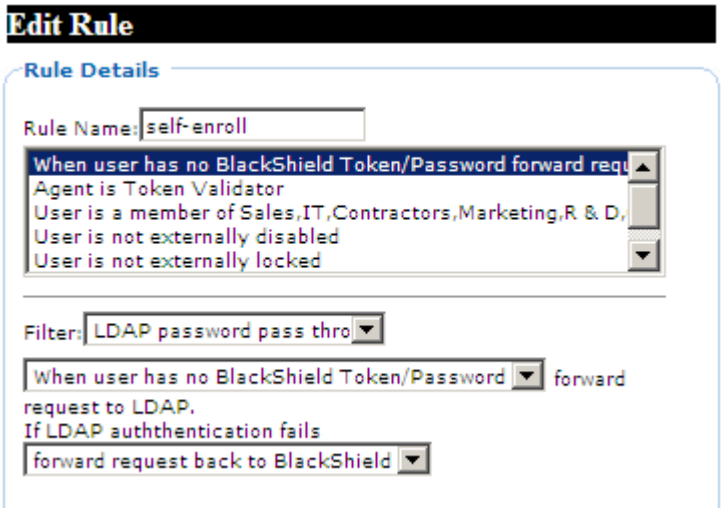
Click “Apply” to save changes.

For detailed post install configuration steps, please refer to the section 'Configuring BlackShield ID' in the BlackShield ID Pro Administrator Guide.

Pre-Authentication Rules

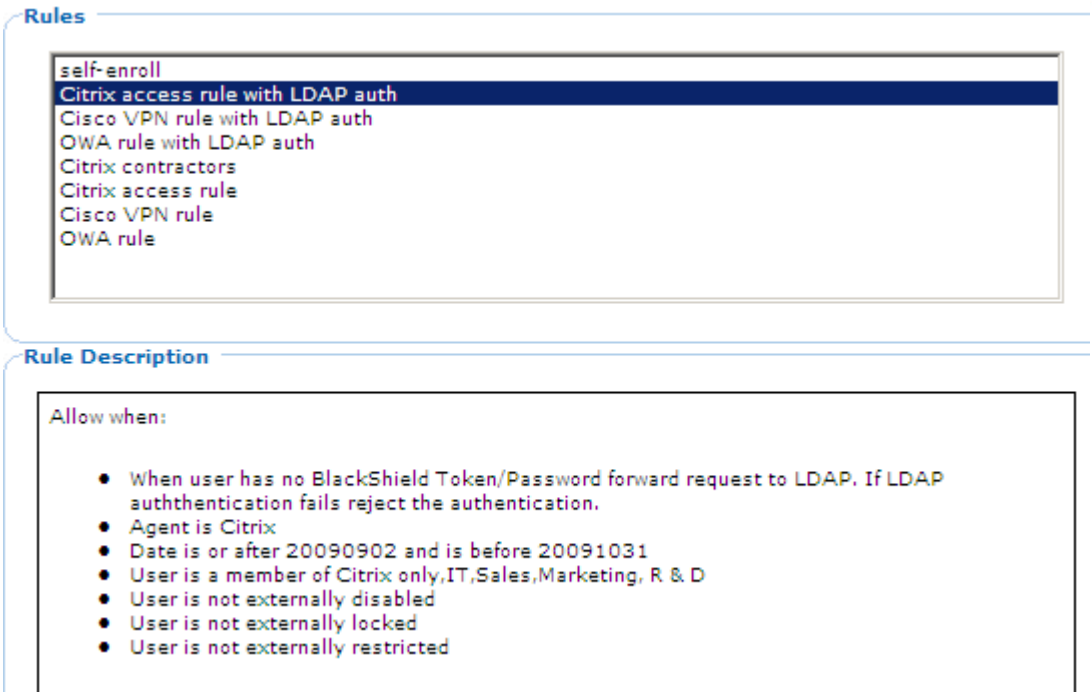
For MyCo to allow for a smooth and seamless transition from static passwords to token based authentication, Pre-Authentication rules need to be added to the BlackShield ID server. This is done via the "System Admin" tab. Click the "Configure" button under the "Pre-Authentication Rules" Section. The goal is to have a set of pre-authentication rules that permit the use of both tokens and static passwords during the migration period. Additionally MyCo would like the ability for use of static passwords to expire at a predetermined date and also have another group of pre-authentication rules allowing token based authentication only to start at the same time the other rules expire.

First, select the "Allow All" Rule and click "Remove". Now we need to add a rule that will permit users to complete self-enrollment of tokens as they are issued from BlackShield ID. Click the Add button and provide a descriptive name for the rule. From the dropdown menu in the Filter section, select LDAP password pass-through.

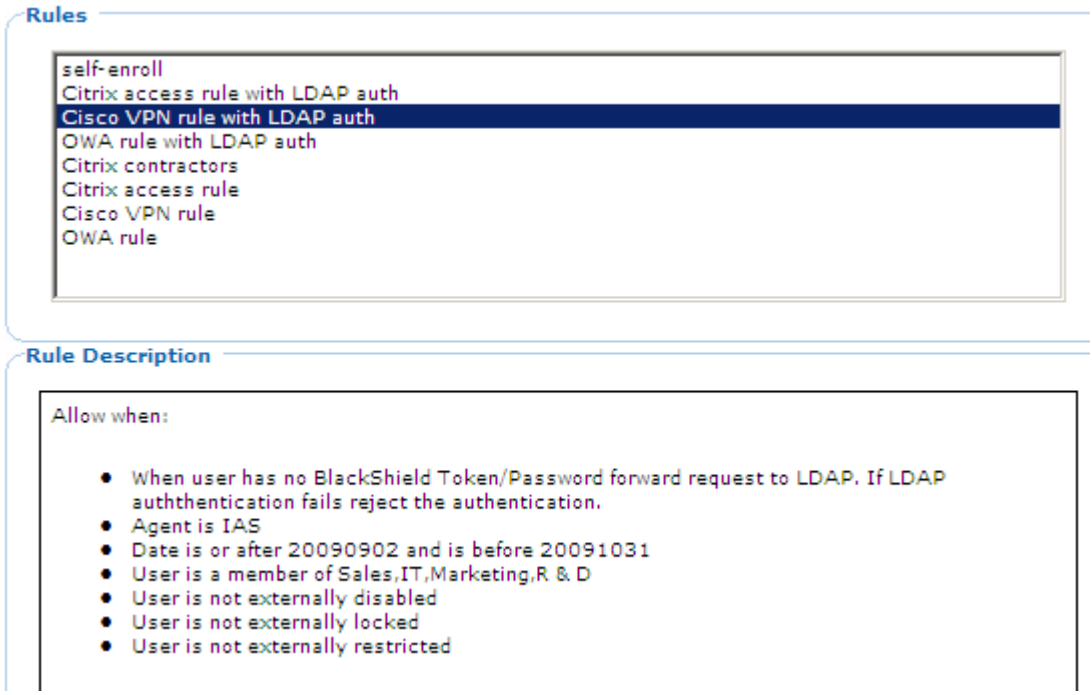


It should be set to "When user has no BlackShield Token/Password", forward request to LDAP, and if LDAP authentication fails "forward request back to BlackShield". The self-enrollment process is done using the Token Validator agent, so it must be added to the pre-authentication rule. To limit the self-enrollment to only those Active Directory groups that contain the users which require tokens, from the Filter dropdown select the option for 'User is a member of' and then add the required Active Directory groups as a comma separated list. In order to have this rule recognise if the users Active Directory account is either locked, disabled or restricted, these filters can be added to the pre-authentication rule. This will cause the self-enrollment for the user to not be successful if their external Active Directory account is locked, disabled or restricted.

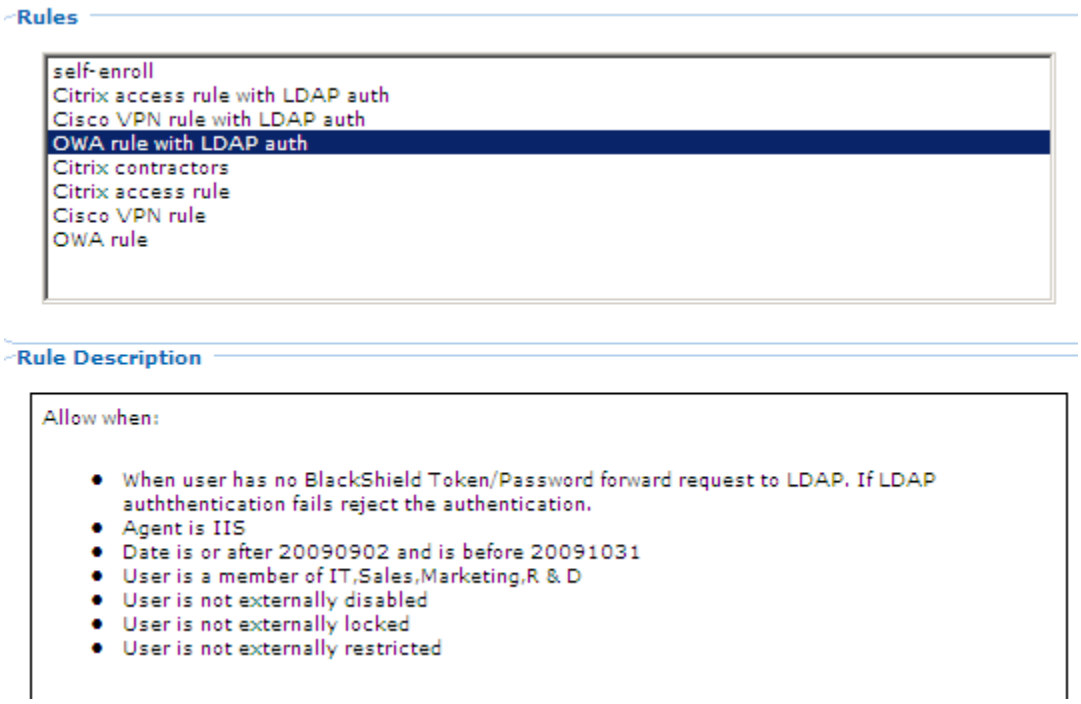
A pre-authentication rule must also be added to permit access via Citrix Web Interface 4.6. This rule permits access with static passwords until the user has completed the self-enrollment of a token, and also restricts access to only those user accounts that are members of specific Active Directory groups. It also respects the condition of the user account being locked, disabled, or restricted within Active Directory. This rule is setup with date restrictions on when it starts and expires.



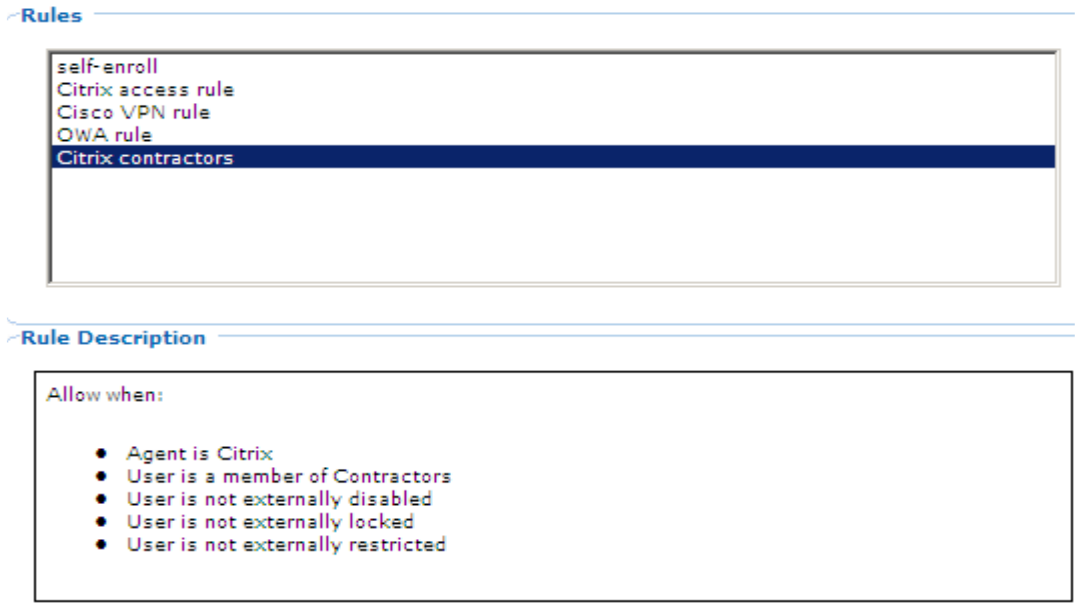
The pre-authentication rule for Cisco VPN access will look like the following:



The OWA (Exchange 2003) rule will have the following settings:

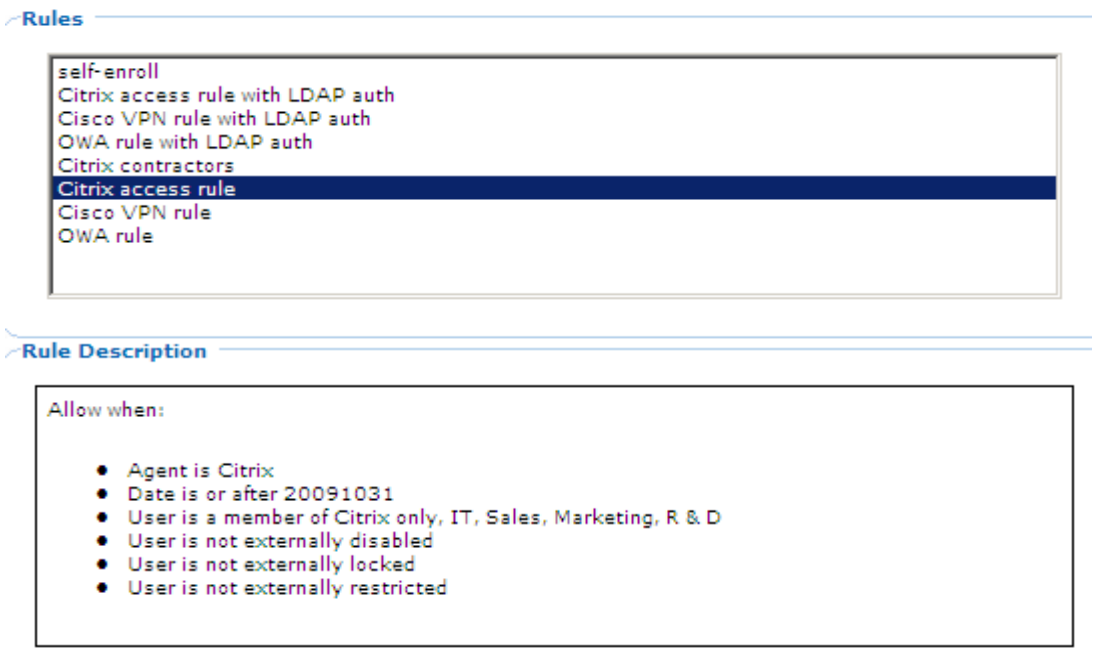


The rule to permit the external Contractors' access via Citrix Web Interface 4.6 with tokens only will have the following settings:

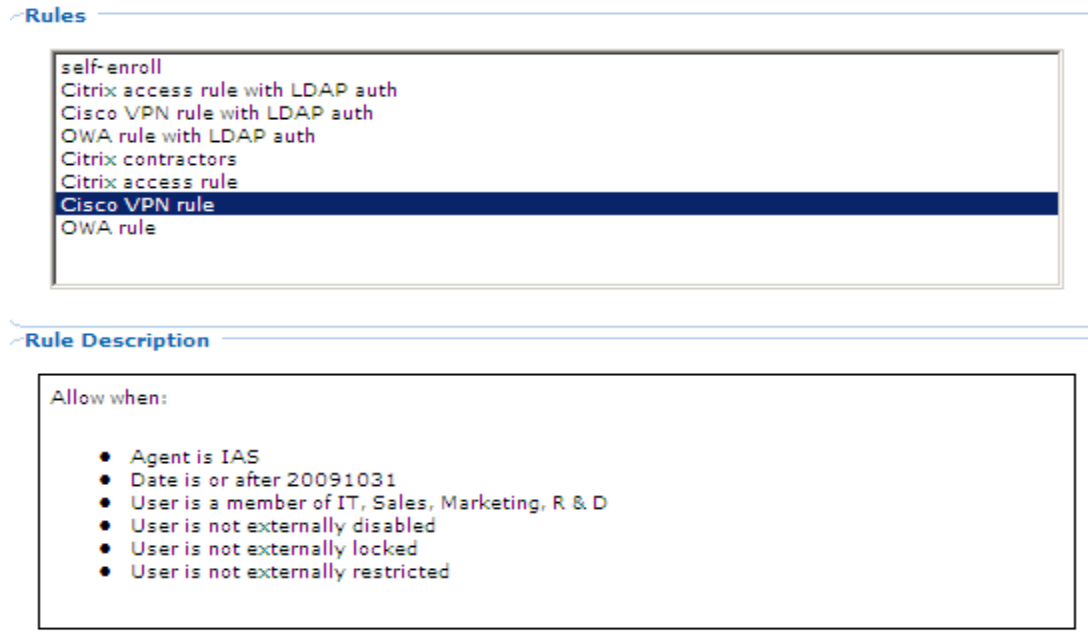


MyCo also needs to create subsequent pre-authentication rules that permit token only authentication and ensure that they are active once the other pre-authentication rules that allow static password access expire. These rules would resemble the following:

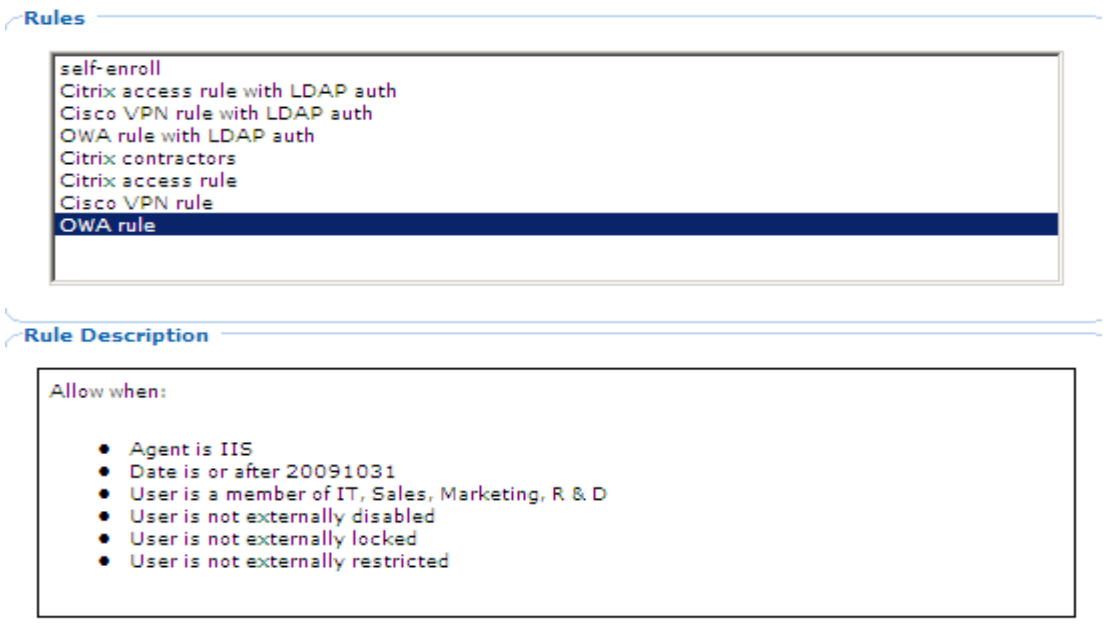
Citrix access rule tokens only:



Cisco VPN rule tokens only:



OWA (Exchange 2003) rule tokens only:



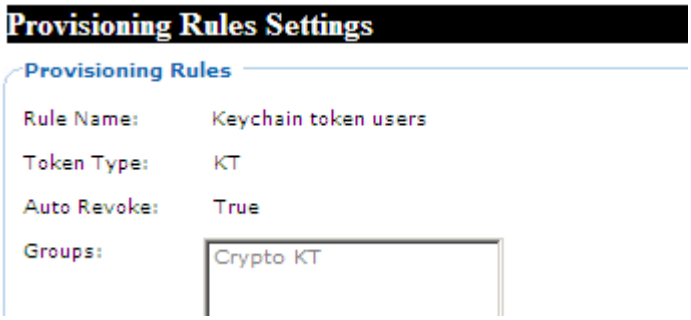
For further details on Pre-Authentication Rules, please refer to the section 'Pre-Authentication Rules' within the 'Advanced Authentication' section in the BlackShield ID Pro Administrator Guide.

Rule Based Provisioning Policy

To allow for a controlled and scheduled deployment of tokens, BlackShield ID can be setup to use rule based provisioning for issuing tokens to users. The provisioning rule automatically issues the chosen token type to user accounts which are members of a specified Active Directory group that is monitored by the provisioning rule. It eliminates the need for security administrators to be occupied with the task of deploying tokens, along with the benefit of establishing a controlled and planned migration from static passwords to token based authentication.

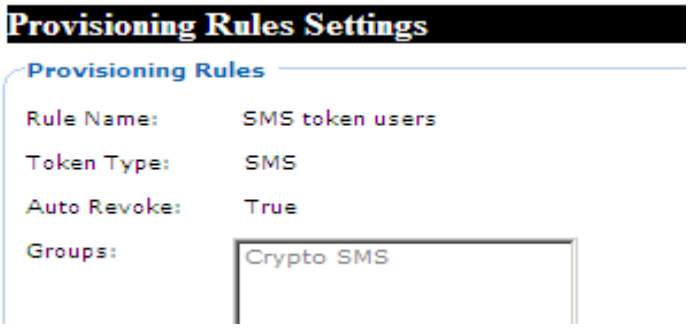
In this scenario, MyCo will be using a combination of hardware (KT) keychain tokens, SMS tokens, and software (MP) based tokens. Therefore three groups will be created within Active Directory, one for KT tokens, one for SMS tokens and one for MP tokens. User accounts will be added to these Active Directory groups in an orderly fashion as the migration to token based authentication is completed. For this scenario the three groups that will be created are to be called 'Crypto KT', 'Crypto MP', and 'Crypto SMS'. Three rule based provisioning entries will be created in BlackShield ID to monitor the above Active Directory groups and issue a token to a user when they have been added to the group. The auto-provisioning delay is set to 5 minutes. Lowering the delay value from 5 minutes to 1 minute will start the provisioning process faster.

i. Rule name: Keychain token users
   - Token type: KT
   - Auto Revoke: enabled
   - AD Group: Crypto KT



ii. Rule name: MP token users
   - Token type: MP
   - Auto remove: enabled
   - AD Group: Crypto MP

iii. Rule name: SMS token users
   - Token type: SMS
   - Auto revoke: enabled
   - AD group: Crypto SMS



For more information on the Provisioning Rules, refer to the 'Rule-Based Provisioning' section in the BlackShield ID Pro Administrator Guide.

Importing Pre-Initialised Tokens

BlackShield ID Pro has the ability to import pre-initialized tokens that can be purchased in batches and imported to the server as required. This removes the need for Security administrators to perform local token initialisation. Once imported, the tokens are ready for deployment to users and have all necessary operating parameters to be available for authentication against the BlackShield ID server.

For further details on importing pre-initialised tokens, see the section on 'Overview of Token Management' in the BlackShield ID Pro Administrator Guide.

5. Testing & Internal Communications

Prior to rolling the token based solution out to MyCo's entire end-user community, steps will be taken to have a subset of the security administrators and IT staff who will be responsible for the management of the BlackShield ID system, to go through the process of testing and documenting the rule based token provisioning and self-enrollment of tokens, along with the login experience with OWA, Citrix Web Interface and Cisco VPN after these remote access devices have been configured for two-factor authentication.

This testing phase will be done in the MyCo lab or test environment so as not to have any impact on the rest of the end-user population or production network. It will allow MyCo to come up with a token deployment strategy, along with instructions and documentation that can be communicated to their end-users. This will guide them through the token self-enrollment registration steps, authenticating with either static passwords or with a token against OWA, Cisco VPN and Citrix Web Interface after two-factor authentication has been enabled. MyCo will take advantage of their own internal notification and communication infrastructure to inform and provide these changes to the end-users.

Furthermore, MyCo will leverage the flexibility of BlackShield ID to customise notification and enrollment messaging by editing some of the numerous customisable email template files included with BlackShield ID. MyCo can change the text content of these files to personalise them for their own organisational needs. For more details on the email template files, please refer to the section 'Customising BlackShield ID' in the BlackShield ID Pro Administrator Guide.

6. Installations

Installing & Configuring BlackShield NPS IAS Agent

The BlackShield Agent for Microsoft Internet Authentication Service (IAS) and Network Policy Server (NPS) enables these RADIUS servers to authenticate against the BlackShield ID Pro server. For MyCo's requirements, enabling IAS / NPS with the BlackShield agent will allow for their implementation of token based authentication with their Cisco VPN infrastructure. Refer to the "Agent_Microsoft_IAS_NPS.pdf" document for installation and configuration information or the 'Installing BlackShield ID Server and RADIUS' section of the BlackShield ID Pro Administrators Guide.

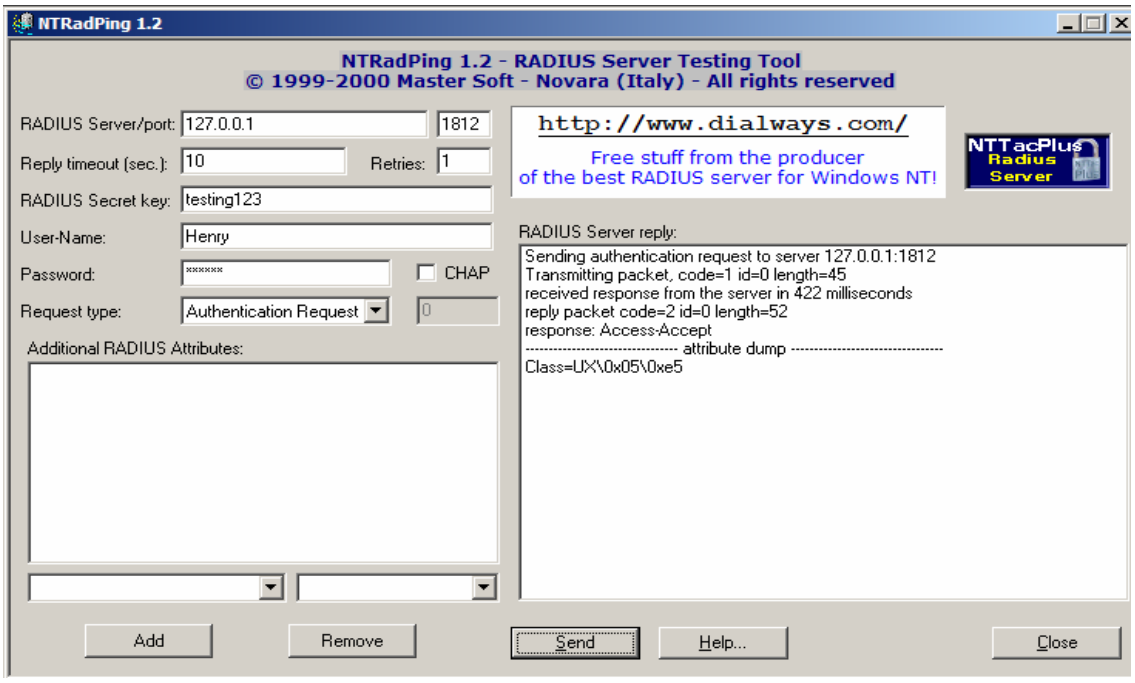
Note: *Create a RADIUS Client for the VPN device authenticating to IAS, and also create a RADIUS client for localhost. The RADIUS client for localhost is used for testing purposes.*

Testing RADIUS Authentication with LDAP Pass-Through

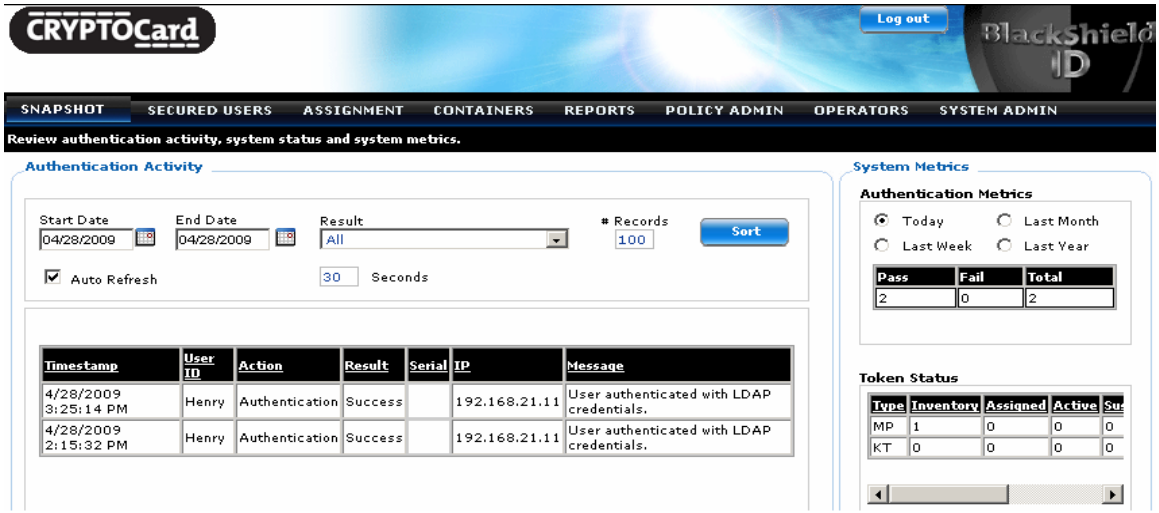
A RADIUS test authentication via localhost should be performed to verify that BlackShield is accepting the authentication.

Launch the NTRadPing tool that comes with the BSID_2.5.zip download.

- Provide the IP address of the RADIUS Server which is 127.0.0.1 in this example
- RADIUS Port is 1812
- RADIUS Shared Secret (must be identical to shared secret entered on IAS / NPS)
- Active Directory username
- Active Directory password



If it succeeds, the Snapshot tab within the BlackShield ID manager will show the authentication success using LDAP credentials.



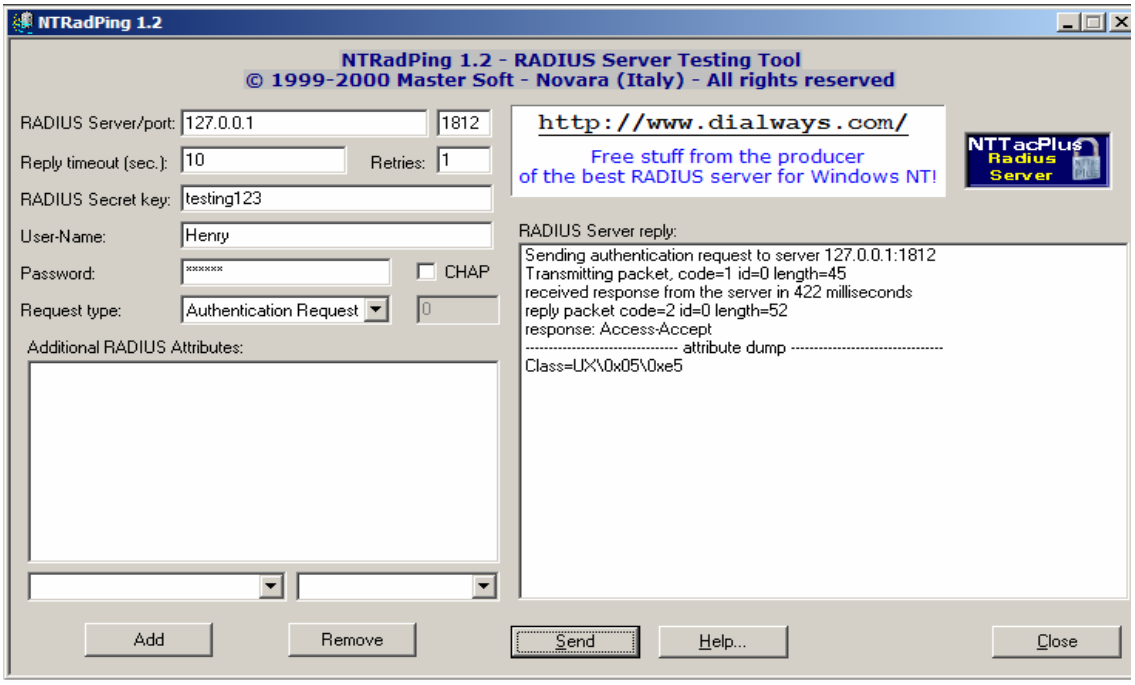
Testing RADIUS Authentication with Token Based Authentication

Following the successful test of the RADIUS authentication using static passwords, a RADIUS test authentication via localhost should be performed with token based authentication to verify that BlackShield is accepting the authentication. MyCo will assign a token to a 'test' user account using the rule based provisioning method.

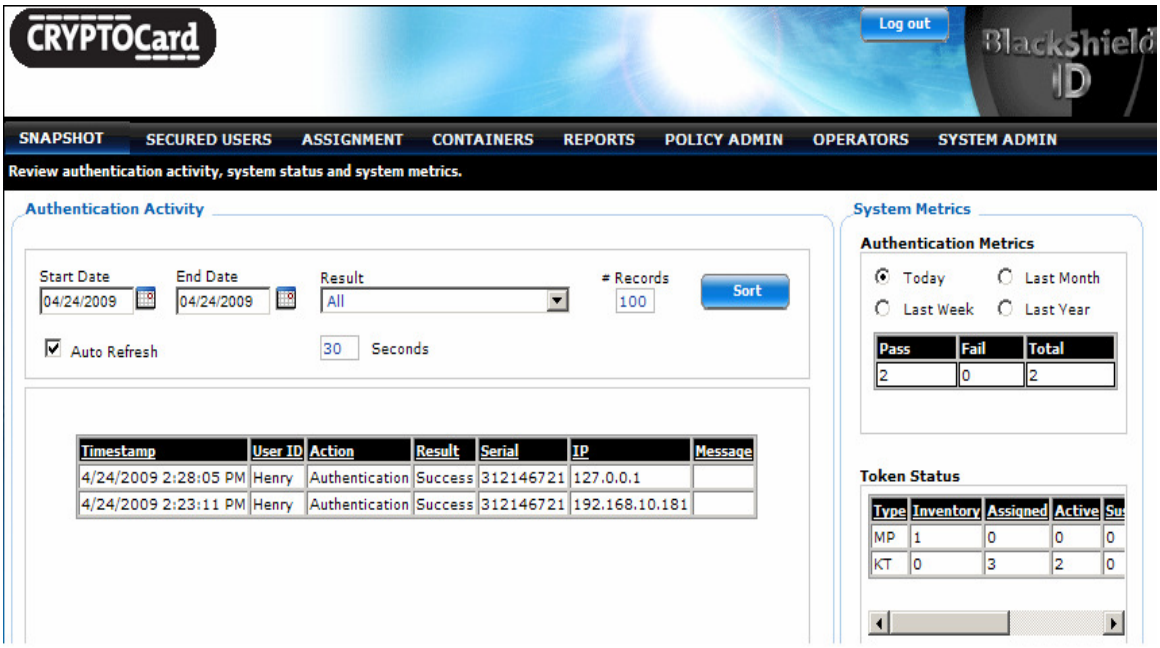
Launch the NTRadPing tool that comes with the BSID_2.5.zip download.

- Provide the IP address of the RADIUS Server which is 127.0.0.1 in this example
- RADIUS Port is 1812
- RADIUS Shared Secret (must be identical to shared secret entered on IAS / NPS)
- Active Directory username
- One-time password provided by a BlackShield token assigned to the user

Note: *depending on the PIN policy associated with the token, the user will need to either enter just the one-time password value generated by the token, or provide a PIN value + the one-time password value generated by the token.*



If it succeeds, the Snapshot tab within the BlackShield ID manager will show the authentication success using token credentials.



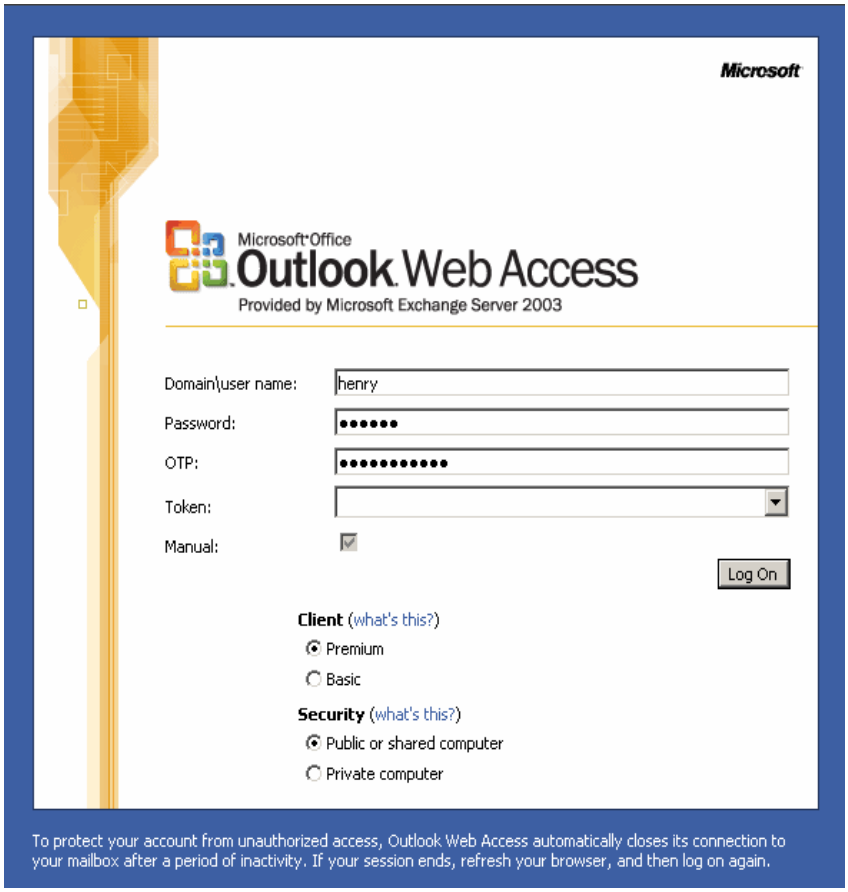
At this stage, MyCo can now configure their test Cisco VPN device to authenticate against BlackShield ID via RADIUS using either static passwords or a token based password. Once the configuration of the Cisco VPN is completed, when presented with the Cisco VPN SSL login page or IPSec client logon dialog box, the 'test' account can provide their Active Directory username and Active Directory password if a token is not currently assigned to the 'test' account. When a token is assigned to the 'test' account, the credentials that must be provided are the Active Directory username and one-time password generated by the token.

Installing & Configuring BlackShield ID IIS 6 Agent

The BlackShield Agent for Microsoft Internet Information Server 6.0 (IIS 6) enhances the login process for Outlook Web Access for Exchange 2003 to require token based authentication against the BlackShield ID Pro server. For MyCo's requirements, enabling IIS 6 with the BlackShield IIS 6 Agent will allow for their implementation of token based authentication with their OWA infrastructure. Refer to the "IIS-BSID.pdf" document for installation and configuration information.

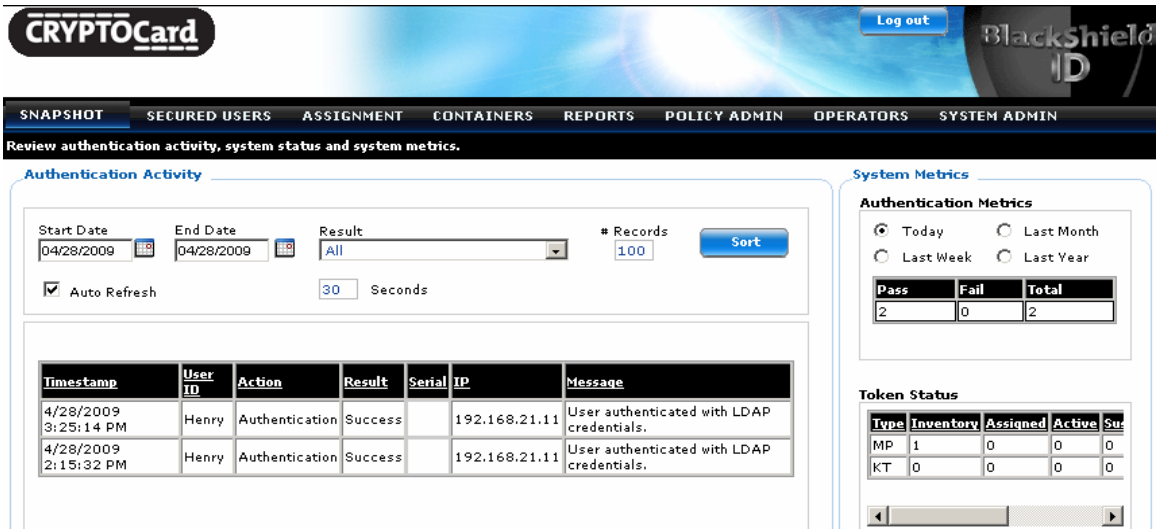
Testing OWA Forms Based Authentication using LDAP Pass Through

After applying CRYPTOCard to protect OWA Forms Based Authentication, navigate to the OWA Forms Based Page externally. The following webpage is displayed:



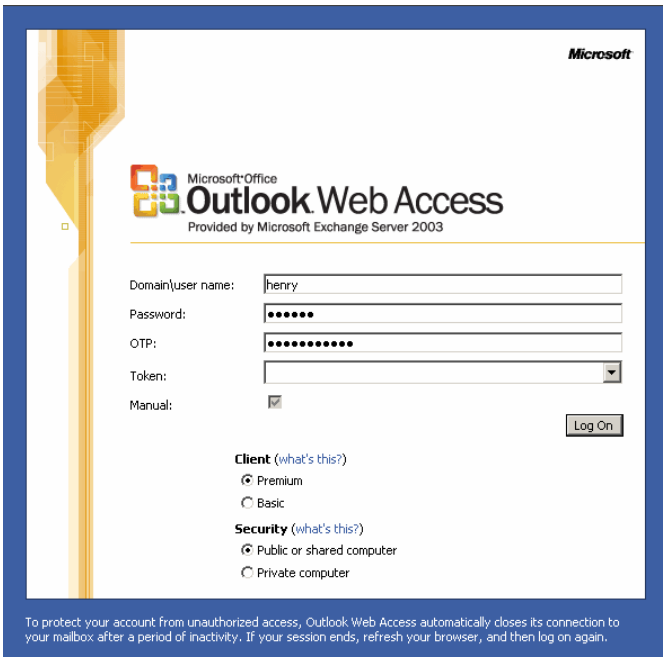
Log in with a 'test' user, and provide their Active Directory credentials. The user will enter their Active Directory Password in the Password and OTP field as they do not have a token assigned to them yet.

If authentication succeeds, the Snapshot tab within the BlackShield ID Manager will display the authentication success.



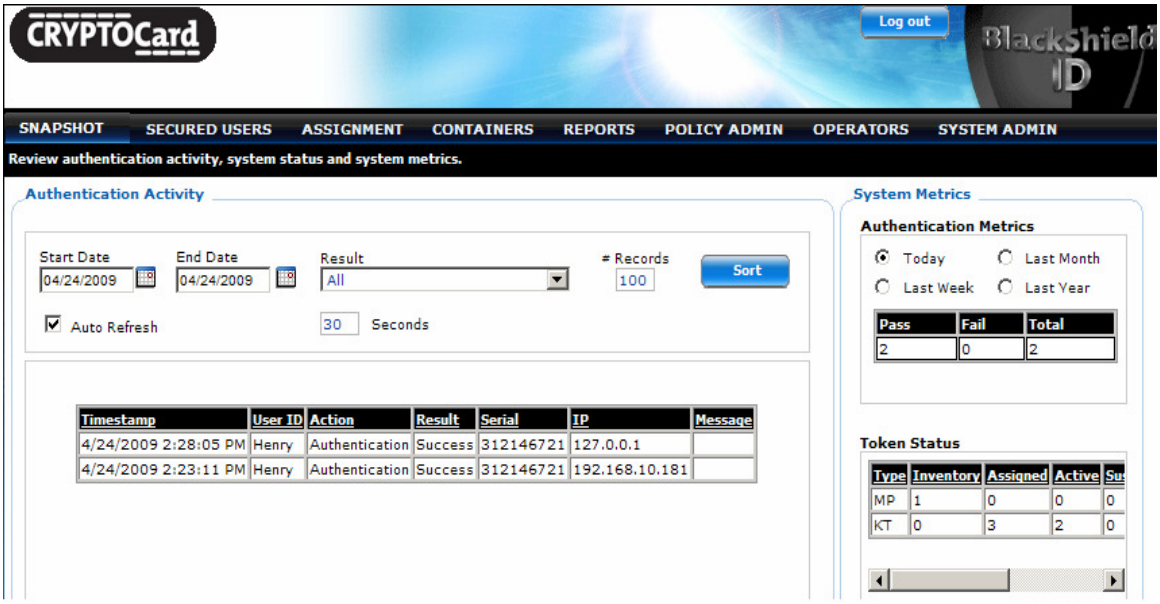
Testing OWA Form Based Authentication with Token Based Authentication

Following the successful test of the OWA authentication using static passwords, a test authentication should be performed with token based authentication to verify that BlackShield is accepting the authentication. MyCo will assign a token to a 'test' user account using the rule based provisioning method. Navigate to the OWA Forms Based Page externally. The following webpage is displayed:



In this example the 'test' user will need to provide their Active Directory user name, their Active Directory password in the Password field, and the one-time password provided by a BlackShield token assigned to the 'test' user in the OTP field.

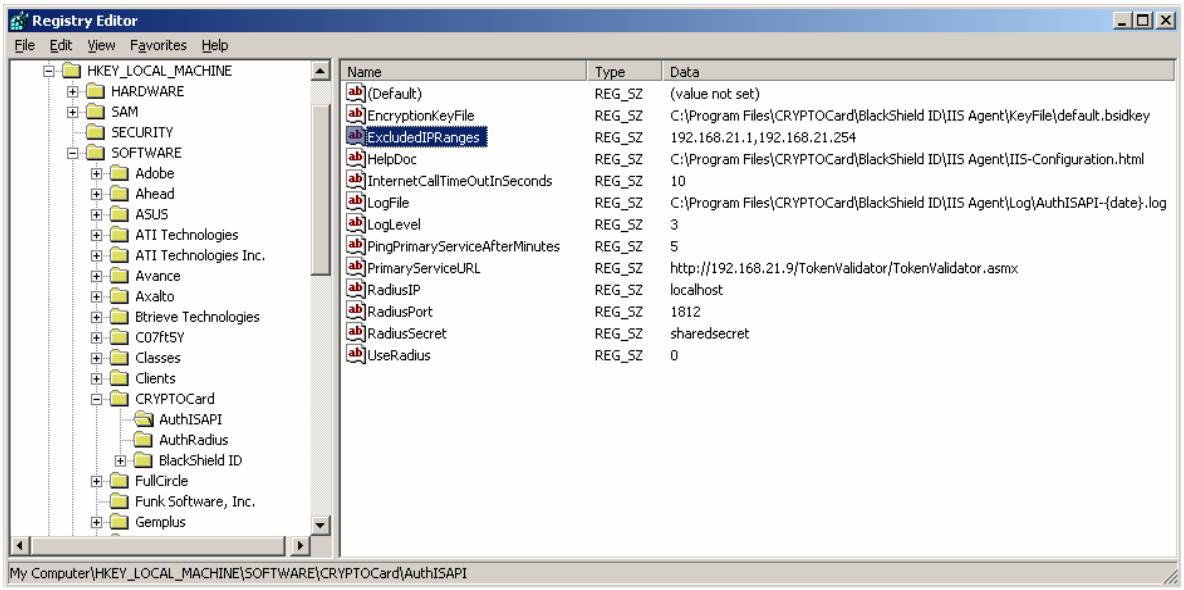
If it succeeds, the Snapshot tab within the BlackShield ID manager will show the authentication success using token credentials.



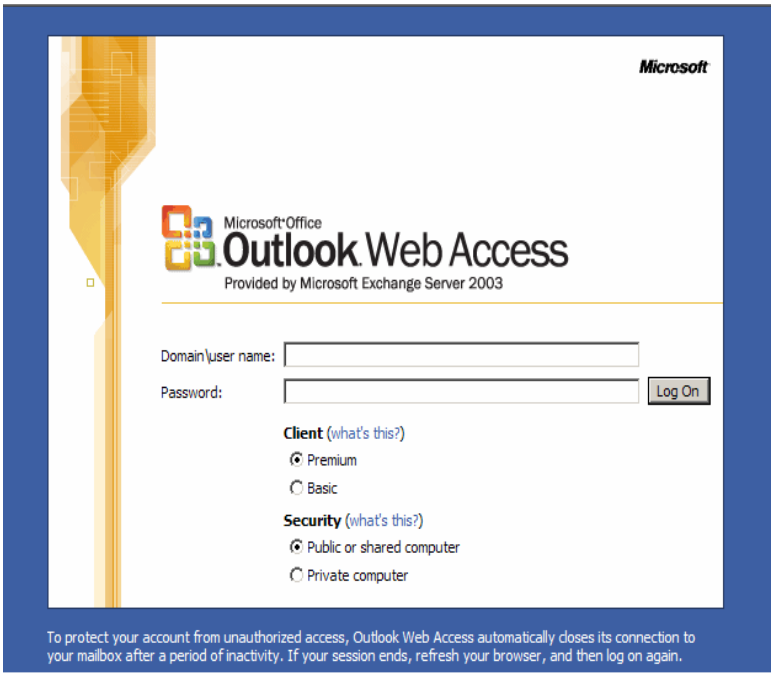
Configure IP Exclusion List for OWA

Since MyCo does not want to enforce token based authentication for their user population when accessing OWA from their internal network, an IP Exclusion List should now be added to the IIS 6 Agent to allow internal end users to access OWA without using Two-Factor Authentication.

- On the IIS 6 / OWA Server, launch “Regedit”
- Go to: \HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthISAPI
- Double Click on the “ExcludedIPRanges” Key on the right hand side
- Add in the internal subnet of the company



After adding the Excluded IP addresses, navigate to the OWA Forms Based webpage internally. The Two-Factor Authentication fields have been omitted from the webpage so users can log in with their normal Active Directory credentials.



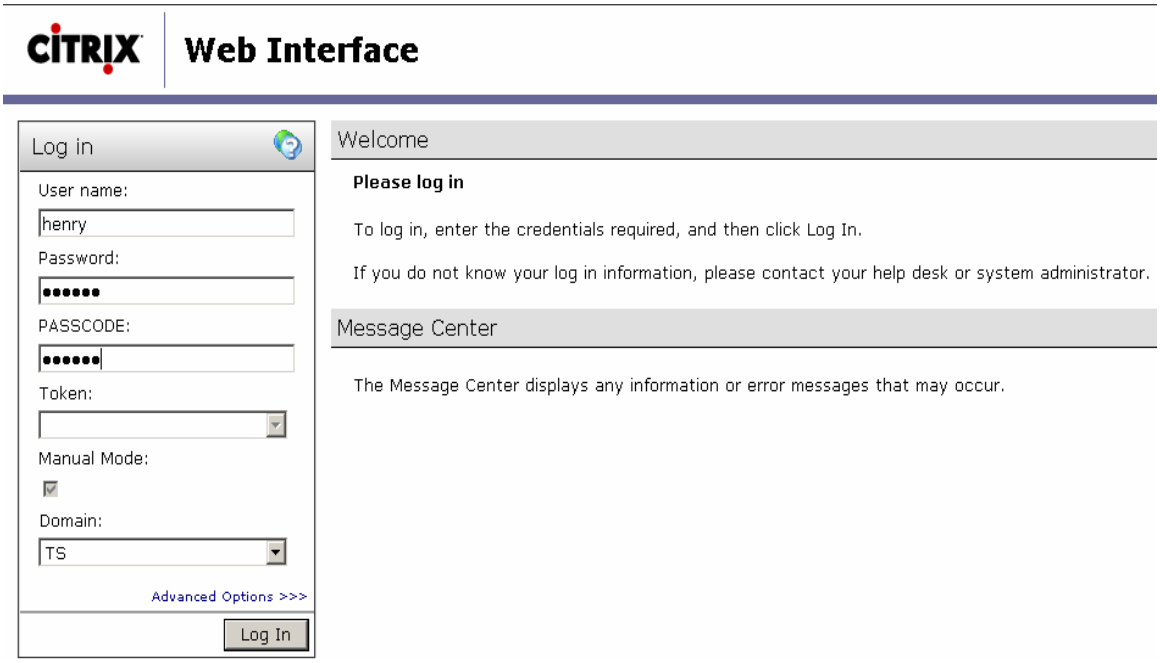
Installing & Configuring BlackShield ID Citrix Web Interface 4.6 Agent

The BlackShield Agent for Citrix Web Interface 4.6 (CWI) strengthens the login process for Citrix Web Interface 4.6 to require token based authentication against the BlackShield ID Pro server. For MyCo's requirements, enabling Citrix Web Interface 4.6 with the BlackShield Citrix Web Interface 4.6 Agent will allow for their implementation of token based authentication with their Citrix Web Interface infrastructure. Refer to the "CitrixWI_4.6.pdf" document for installation and configuration information.

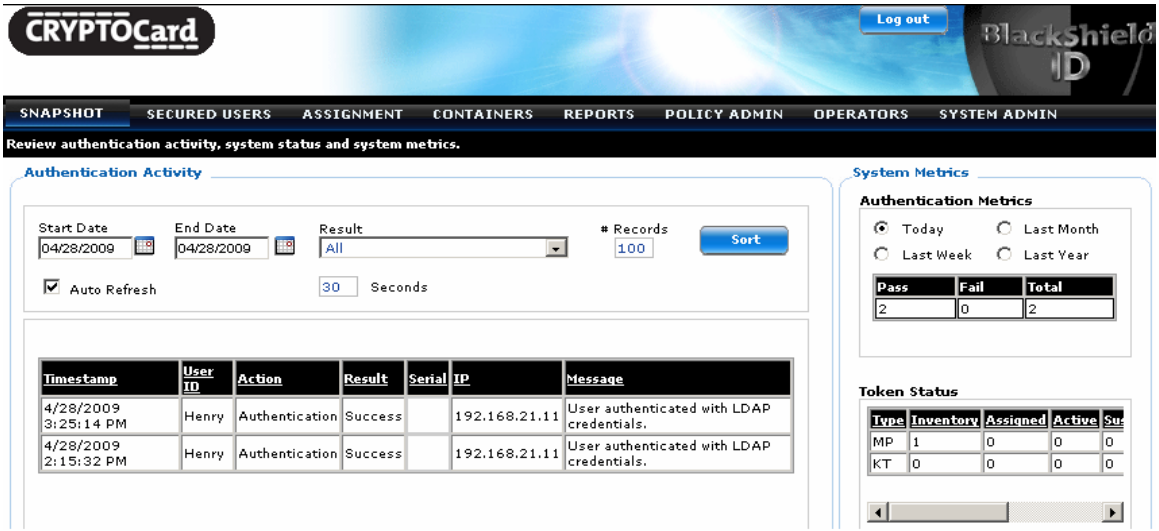
Testing Citrix Web Interface 4.6 using LDAP Pass Through

After installing the BlackShield ID Citrix Web Interface 4.6 Agent, navigate to the Citrix Web Interface 4.6 webpage. The webpage has been changed to now have a Passcode and Token field, along with a manual checkbox.

Log in with a 'test' user, and provide their Active Directory credentials. The user will enter their Active Directory user name and then their Active Directory password twice – once in the Password field and then in the Passcode field as they do not have a token assigned.



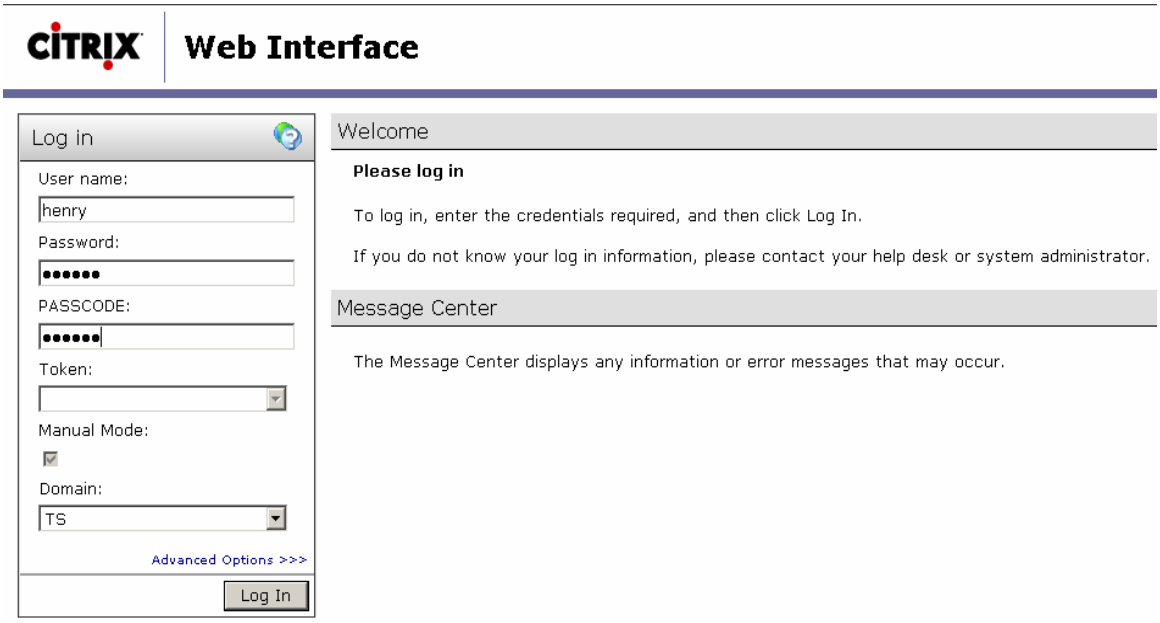
If authentication succeeds, the Snapshot tab within BlackShield ID Manager will display the successful authentication.



Testing Citrix Web Interface Authentication with Token Based Authentication

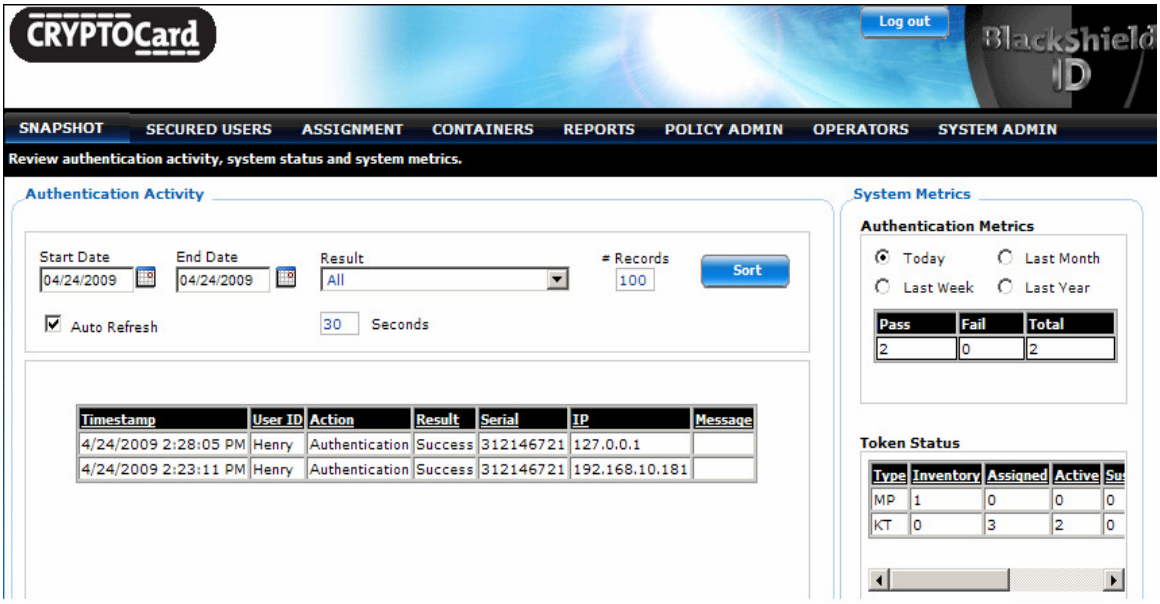
Following the successful test of the Citrix Web Interface authentication using static passwords, a test authentication should be performed with token based authentication to verify that BlackShield is accepting the authentication. MyCo will assign a token to a 'test' user account using the rule based provisioning method.

Navigate to the Citrix Web Interface login page.



In this example the 'test' user will need to provide their Active Directory user name, their Active Directory password in the Password field, and the One-Time Password provided by a BlackShield token assigned to the 'test' user in the PASSCODE field.

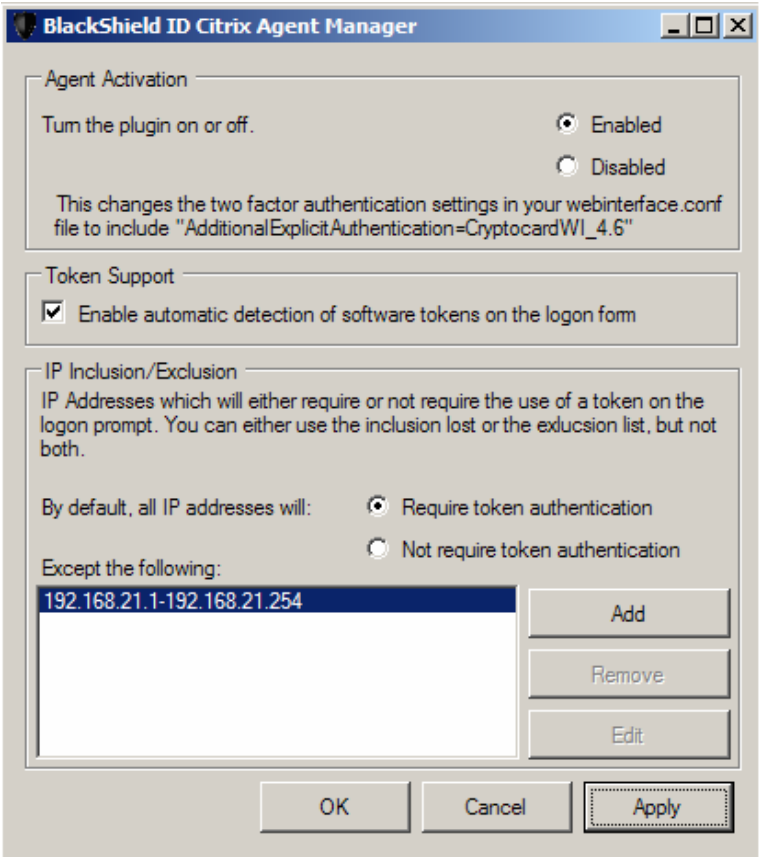
If it succeeds, the Snapshot tab within the BlackShield ID manager will show the authentication success using token credentials.



Configure IP Exclusion List for Citrix Web Interface 4.6

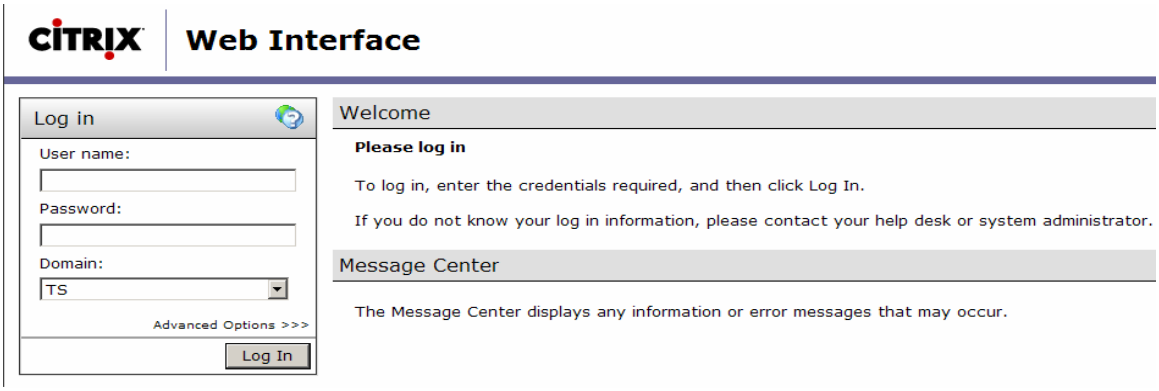
Since MyCo does not want to enforce token based authentication for their user population when accessing Citrix Web Interface from their internal network, an IP Exclusion List should now be added to the IIS 6 Agent to allow internal end users to access Citrix Web Interface without using Two-Factor Authentication.

- On the Citrix Web Interface server launch the BlackShield ID Citrix Agent Manager
- To add an IP Exclusion, click the Add button
- Enter the exclusion in the format that is displayed in the popup box
- Select OK to add the IP Exclusion
- Click OK when finished



Note: *By default, all options within the BlackShield ID Citrix agent Manager are turned on.*

After adding in the IP Exclusion, navigate to the Citrix Web Interface 4.6 webpage internally. The Two-Factor Authentication fields have been removed from the webpage so internal users can log in with their normal Active Directory Credentials.



And with these final steps complete, the BlackShield ID solution is now fully configured, tested and operational.

Conclusion

Now that we have reached the end of the implementation for MyCo, we hope you have found this Guide useful and beneficial in understanding how easily and seamlessly BlackShield ID can fit in to your organisation's security framework.

As this Best Practice Guide was representative of a complex case study implementation, if there were any areas within this document that either did not address some of your own specific requirements or if you would like a deeper understanding of any of the features and functionalities you saw, we would be happy to provide you with our comprehensive BlackShield ID Pro Administrator Guide.

Finally please feel free to get in touch with either your CRYPTOCard Representative or our Technical Support Team to talk through any requirements and queries:

t: +1 800 30707042
e: support@cryptocard.com